THE CHANGING CHARACTER OF WAR: RECOMMENDATIONS FOR COMPETING WITH RUSSIA IN THE INFORMATION AGE

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
Art of War Scholars

by

NICHOLAS J. KANE, MAJ, USA
B.A., Lehigh University, Bethlehem, Pennsylvania, 2003

Fort Leavenworth, Kansas
2018

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-06-2018	Master's Thesis	AUG 2017 – JUN 2018

4. TITLE AND SUBTITLE

The Changing Character of War: Recommendations for Competing with Russia in the Information Age

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Nicholas J. Kane

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In the Information Age, nation-states compete in the space between peace and declared conflict. The most significant instrument of national power in this space is information. Russia is more able to dynamically operate in the Information Environment (IE) than the United States. Russia leveraged the information instrument of national power in Crimea and Eastern Ukraine to set conditions for overt military action. Russian New Generation Warfare activities in Ukraine from 2013-2017 frame threats the United States faces from Russia in the IE, both in the gray zone and in the event of large-scale combat operations. The fundamental problem facing the Department of Defense ability to support a whole-of-government approach to competition with Russia in the IE is a misunderstanding of information operations and the IE. Some areas in which capability gaps exist that contribute to this misunderstanding are doctrine, organization, and leadership education. Reforms in these three areas can significantly improve the defense enterprise's understanding of information and operating in the IE.

15. SUBJECT TERMS
Russia, Information Operations, Ukraine, New Generation Warfare, Doctrine, Organization, Education, USCYBERCOM

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	112	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Nicholas J. Kane

Thesis Title: The Changing Character of War: Recommendations for Competing with Russia in the Information Age

Approved by:

_____, Thesis Committee Chair
LTC Andrew K. Murray, M.A.

_____, Member
LTC Philip D. Martin, M.A.

_____, Member
David W. Mills, Ph.D.

Accepted this 15th day of June 2018 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

ABSTRACT

THE CHANGING CHARACTER OF WAR: RECOMMENDATIONS FOR COMPETING WITH RUSSIA IN THE INFORMATION AGE, by MAJ Nicholas J. Kane, 112 pages.

In the Information Age, nation-states compete in the space between peace and declared conflict. The most significant instrument of national power in this space is information. Russia is more able to dynamically operate in the Information Environment (IE) than the United States. Russia leveraged the information instrument of national power in Crimea and Eastern Ukraine to set conditions for overt military action. Russian New Generation Warfare activities in Ukraine from 2013-2017 frame threats the United States faces from Russia in the IE, both in the gray zone and in the event of large-scale combat operations. The fundamental problem facing the Department of Defense is its ability to support a whole-of-government approach to competition with Russia in the IE because the DoD has not adequately framed what constitutes information operations and the IE. Capability gaps related to doctrine, organization and leadership education also contribute to the DoD's inability to compete with Russia in the IE. Reforms in these three areas can significantly improve the DoD's understanding of information and operating in the IE.

ACKNOWLEDGMENTS

First and foremost, I must thank my wife Catherine for her love and support during this journey. My thesis committee: LTC Andrew Murray, Dr. David Mills, and LTC Philip Martin, for their guidance and accountability; my fellow Art of War Scholars, specifically MAJs Ariel Schuetz, Kwonwoo Kim, and Maj. Josh "Sauce" Singsaas, and Dr. Dean Nowowiejski, for their candor, encouragement, and considerable feedback. Mr. Timothy Thomas, who set me on the first steps of this journey. Dr. David Spurlin for assisting with instrument development and the Institutional Review Board process, and Mrs. Bobbie Murray for schooling me on Human Subjects Research. Ms. Venita Kruger, for her editorial services. Ms. Amanda Hemmingsen for a significant azimuth check. MG "Skip" Davis, COL Mike Jackson, COL Mark Vertuli, LTC Amy Burrows, and MAJ Jerome Petersen who devoted their time and perspective during interviews, which certainly made this a better thesis. Finally, I want to thank everyone else who touched this project and facilitated my completion.

TABLE OF CONTENTS

Page

ACRONYMS

C2	Command and Control
C2W	Command and Control Warfare
CGSC	Command and General Staff College
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
DoD	Department of Defense
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership Education, Personnel, Facilities, and Policy
EW	Electronic Warfare
GEC	Global Engagement Center
IE	Information Environment
IO	Information Operations
IRC	Information Related Capability
IW	Information Warfare
JIOWC	Joint Information Operations Warfare Center
MILDEC	Military Deception
MISO	Military Information Support Operations
NATO	North Atlantic Treaty Organization
NGW	New Generation Warfare
OPSEC	Operations Security
PA	Public Affairs
PME	Professional Military Education
USCYBERCOM	United States Cyber Command

USINFOCOM	United States Information Command
USG	United States Government

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER 1

INTRODUCTION

> [The] Information age is changing the essence and content of modern war.[1]
>
> — V.K. Novikov and S.V. Golubchikov
> "Color Revolutions in Russia"

> There has never been a time in our history when there was so great a need for our citizens to be informed and to understand what is happening in the world. The cause of freedom is being challenged throughout the world today and propaganda is one of the most powerful weapons they have in this struggle. Deceit, distortion, and lies are systemically used by them as a matter of deliberate policy[.][2]
>
> — Harry S. Truman,
> "Address on Foreign Policy"

Overview

The United States Department of Defense (DoD) is in the midst of a military revolution fueled by globalization, advancements in technology, and expanded access to information. The Information Age has recast society, the military, and the operational environment in which states fight wars. It has also changed how people view power. Joseph Nye and William Owens state:

> Traditional measures of military force, gross national product, population, energy, land, and minerals have continued to dominate discussions of the balance

[1] В.К. Новиков, С.В. Голубчиков, Вестник, Вестник, 3 (60), 2017, стр. 10-16. [V. K. Novikov and S. V. Golubchikov, "Color Revolutions in Russia: Possibility and Reality," *Vestnik,* 3 (60) (2017): 10-16].

[2] Harry S. Truman, "Address on Foreign Policy at a Luncheon of the American Society of Newspaper Editors," 20 April, 1950, accessed 29 April, 2018, http://www.presidency.ucsb.edu/ws/index.php?pid=13768.

of power. These power resources still matter, and American leadership continues to depend on them as well as on the information edge.[3]

The Secretary of Defense, General (Retired) James Mattis, issued guidance stating that the force must modernize.[4] Significant to this modernization is an understanding of the Information Environment (IE) and how the military can operate within it in concert with other Federal agencies across all the instruments of national power (Diplomatic, Informational, Military, and Economic) to achieve strategic, operational, and tactical objectives.

Amidst this military revolution, many of United States' adversaries seized the initiative in the information environment. In his memorandum, Secretary Mattis specifically addresses that "Russia has violated the borders of nearby nations and seeks veto power over the economic, diplomatic, and security decisions of its neighbor."[5]

In a multipolar world, Russia has found significant success leveraging Information in the Crimean Peninsula and Eastern Ukraine to set conditions for military activities in 2013 and 2014. Exploiting commonalities in language, religion, ethnicity, and other aspects of culture, Russia conducted propaganda, deception, and other information and political warfare activities prior to covert military forces influencing populations to actively and passively supported annexation of Crimea and the invasion of

---

[3] Joseph S. Nye and William A. Owens, "America's Information Edge," *Foreign Affairs,* March 1996, accessed 25 April, 2018, https://www.foreignaffairs.com/articles/united-states/1996-03-01/americas-information-edge.

[4] Secretary of Defense, *Guidance from Secretary Jim Mattis* (Washington, DC: Government Printing Office, October 2017), 1.

[5] Ibid.

areas Donetsk and Luhansk oblasts in Eastern Ukraine.[6] This case served to frame the threat that exists from Russia in the IE.

To achieve advantages in the IE, the DoD must bridge gaps in synchronization of information efforts, develop mechanisms to promote unified action in the IE, foster a shared understanding of Information Operations (IO), and embrace changes caused by the Information Age military revolution. This reform will require changes to policy, military doctrine, organizational structures, training, and leadership education of military personnel across the defense enterprise. To support this thesis, the researcher aimed to understand the evolution of IO doctrine, current organizational structures, and education on IO to identify capability gaps and make recommendations for change in these three areas.

Background

The 2014 Ukrainian crisis stems from historical Russian involvement in the area since the mid-17th century. The arguable catalyst for the 2014 downward spiral of the Ukrainian situation was the decision by Ukrainian President Viktor Yanukovych not to sign an association agreement with the European Union that would lead to membership. Russian economic pressure placed upon Yanukovych influenced this decision.[7] After popular protests in which security forces killed civilians, Ukraine's parliament removed Yanukovych as president and subsequent elections put Petro Poroshenko in the

[6] Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Washington, DC: Institute for the Study of War, 2015), 7.

[7] Marcel Van Herpen, *Putin's Wars: The Rise of Russia's Imperialism*, 2nd ed. (New York: Rowman and Littlefield, 2015), 243.

presidential seat of power in Ukraine. He signed the association agreement which was a significant step towards European Union membership. This move set Russian activity in motion that characterized New Generation Warfare (NGW), called New-Type Warfare by the Russians. To understand NGW, one must first understand the various instruments and elements of power that nation-states employ to achieve national objectives.

Definitions

To set a common understanding of terms used in this thesis, below are three significant terms that must be codified at the beginning to mitigate confusion:

Information Environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The IE consists of three dimensions: physical, informational, and cognitive.[8]

Information Operations. The integrated employment, during military operations, of information-related capabilities, in concert with other lines of operation, to influence, disrupt, corrupt, or usurp the decisionmaking of adversaries, or potential adversaries, while protecting our own.[9]

Instruments of National Power: Diplomatic, Informational, Military, Economic. These terms represent the U.S. instruments of national power.[10]

---

[8] Joint Chiefs of Staff, Joint Publication (JP) 3-13, *Information Operations*, change 1 (Washington, DC: Government Printing Office, 2014), ix.

[9] Ibid.

[10] Joint Chiefs of Staff, Joint Publication 1-0, *Doctrine for the Armed Forces of the United States* (Washington, DC: Government Printing Office, 2013), I-12.

Concept of Power

Governments are employing smart power when conducting statecraft today which is the balanced combination of hard and soft power to achieve national objectives. Much of this statecraft demonstrated by Russia borders on warfare, especially conflict within the "gray zone," pre-war space in the spectrum of military conflict. According to Alexander Velez-Green, a researcher focused on Russian military doctrine and though, Russia already views itself as being at war with the U.S, using a whole-of-nation approach and use of securitized media.[11] LTG (R) James Dubik describes the gray zone as "the hostile or adversarial interactions among competing actors below a threshold of conventional war and above the threshold of peaceful competition."[12] One could argue that Russia already views itself as being at war with the U.S., using a whole-of-nation approach to competition with the West and Russia's use of securitized media.

In support of a broad U.S. whole-of-government effort, the DoD must be trained, equipped, and prepared to counter such activities in this uneasy, steady-state environment traditionally referred to as phase zero.[13] To understand how to support unified action, one must first understand the various concepts of power that exist at the state level. Hard and soft power, smart power, and sharp power refer to how a state employs the instruments of national power in an integrated manner to achieve strategic objectives.

---

[11] Alexander Velez-Green, "The United States and Russia Are Already at War," *Small Wars Journal*, accessed 26 April, 2018, http://smallwarsjournal.com/jrnl/art/the-united-states-and-russia-are-already-at-war.

[12] James Dubik and Nic Vincent, *America's Global Competitions: The Gray Zone in Context* (Washington, DC: Institute for the Study of War, 2018), 9.

[13] Department of Defense, *Strategy for Operations in the Information Environment* (Washington, DC: Government Printing Office, 2016), 5.

Table 1. Types of Power

Type of Power	Description	Typically used instruments of DIME
Soft Power	Instruments used to influence with attraction	**D and I**
Hard Power	Instruments used to influence with coercion	**M and E**
Smart Power	Integrated employment of all the instruments of power, hard and soft	**D I M E**
Sharp Power	Use of soft power instruments for deceptive and coercive purposes	**D and I**

Source: Created by author.

Joseph Nye stated that he developed the term smart power to, "counter the misperception that soft power alone can produce effective foreign policy." He continued, "smart strategies that combine the tools of both hard and soft power" are necessary.[14] Nye further defined, "power is one's ability to affect the behavior of others to get what one wants. There are three basic ways to do this: coercion, payment, and attraction. Hard power is the use of coercion and payment. Soft power is the ability to obtain preferred outcomes through attraction."[15]

[14] Joseph P. Nye, "Get Smart-Combining Hard and Soft Power," *Foreign Affairs* 88, no. 4 (July/August 2009): 160-163.

[15] Ibid.

By projecting smart power, Russia displayed significant aggression that has yet to cross the threshold to kinetic conflict with North Atlantic Treaty Organization (NATO) members. Given the perceived conventional military advantage the U.S. currently maintains, it is not likely Russia will choose to engage in overt conflict with NATO members in the near term. Instead, Russia will continue to weaponize ideas, employ new capabilities and tactics in the IE, and leverage a whole of nation approach to project smart power in states along its Western "front." The Russian "whole of nation" approach incorporates commercial and criminal entities as well as transnational actors in addition to the instruments of national power. This employment of power will cause neighboring states and other world powers to reevaluate their ability to compete with Russia in the IE, in the author's opinion.

From the U.S. perspective, awareness exists of the threats posed by Russia, but lack of proactivity and timely responsiveness in the IE make it difficult to gain and maintain the initiative in the narrative space. Bureaucracy and statutes also impede efforts to mitigate the mismatch in dominance in the IE. Efforts are currently underway to ameliorate the identified gaps such as Congress's allocation of additional funds to counter propaganda efforts by Russia and China in the Countering Foreign Disinformation and Propaganda Act of 2016.[16] Notably, then-Secretary of Defense Ash Carter signed the *Strategy for Operations in the Information Environment* in July 2016 as part of the DoD effort to compete with Russia and other state and non-state actors in the IE.[17]

---

[16] U.S. Congress, House, *Countering Foreign Propaganda and Disinformation Act of 2016*, H.R.5181.

[17] Department of Defense, *Strategy for Operations in the Information Environment*.

Problem Statement

The U.S. must address capability gaps within the defense enterprise that prevent more effective approaches to achieving advantages in the IE. The prevalent problem that results from these gaps is a fundamental misunderstanding of IO, and how to understand, plan for, and execute operations in the IE in concert with operational and strategic campaigns. Based on GEN Philip Breedlove's assessment, "neither the United States' military nor those of its allies are adequately prepared to rapidly respond to overt [Russian] military aggression.[18] Nor are they sufficiently ready to counter the kind of hybrid warfare that Moscow has waged in eastern Ukraine."[19] This hybrid warfare mentioned by GEN Breedlove refers to Russian "new-type warfare" or what some call "NGW." In 2015, General Sir Nicholas Houghton, then Chief of the Defence Staff of the British Armed Forces, addressed this in a speech, "Russia now presents a threat in more novel ways to several of our NATO allies; and potentially, if not handled well, to the coherence of NATO as an Alliance. In some of our responses we must be careful not to assume that Russia's rationality mirrors our own."[20] If left unchecked, Russian activity may lead to destabilization of NATO and U.S. relationships and undermine U.S. global

---

[18] General Breedlove was the EUCOM commander and Supreme Allied Commander in Europe from 2013-2017.

[19] Philip M. Breedlove, "How to Handle Russia and Other Threats," *Foreign Affairs*, 13 June 2016, accessed 25 April, 2018, https://www.foreignaffairs.com/articles/europe/2016-06-13/natos-next-act.

[20] Nicholas Houghton, "Building a British Military Fit for Future Challenges Rather Than Past Conflicts" (Transcript of speech made by General Sir Nicholas Houghton, Chatham House, London, 15 September 2015), 4, accessed 25 April 2018, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150901-Chatham%20House%20Speech-O.pdf.

power through influencing foreign elections, dissemination of false news and rumors to create social, political, and economic unrest. Furthermore, the 2018 National Defense Strategy states: [21]

> Some competitors and adversaries seek to optimize their targeting of our battle networks and operational concepts, while also using other areas of competition short of open warfare to achieve their ends (e.g., information warfare, ambiguous or denied proxy operations, and subversion). These trends, if unaddressed, will challenge our ability to deter aggression.

United States values, laws, and Constitution preclude the military from leveraging information related capabilities in a manner that can dynamically compete with and defeat Russia in the IE. This adherence to democratic values will not change as freedoms of speech and of the press [information] are founding principles of the United States.

Primary Research Question

The aim of this research is to answer the following question: Are DoD reforms necessary to support a whole of government approach to competition with Russia in the IE? This question is vital to determine how the U.S. defense enterprise can address Russian threats as part of the broader United States' Government (USG) effort.

Secondary Research Questions

To arrive at a satisfactory answer to this question, additional research must first also answer two secondary questions that will highlight the threats in the IE and focus analysis on DoD gaps in addressing threats:

[21] Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: Government Printing Office, 2018), 3.

1. How did Russia leverage the information instrument of national power in conjunction with the military in Ukraine?
2. What capability gaps can the DoD address to maximize effectiveness to address threats in the information environment?

Significance of Study

There is a lack of fundamental knowledge within the joint force about what IO is. Colonel Mark Vertuli, an IO officer serving at United States Strategic Command, and other interviewees echoed this opinion. "Cyber" and "IO" become nebulous activities to commanders and staffs because of the abstractness of the cognitive dimension of the IE and the technical capabilities that can achieve desired effects in the physical and informational dimensions of the IE. This confusion derives from a general misunderstanding of the IE, what the different Information Related Capabilities (IRCs) can do, and ambiguity in policy and doctrine specifically related to terminology. This study proffers recommendations to mitigate confusion through refined doctrine and advocating for better education of the force.

The DoD Strategy for Operations in the Information Environment highlights the importance of IO:[22]

> Information operations are an important component of military operations and in all phases of an operation or campaign, including shaping activities in the steady-state. The ability to monitor, characterize, and analyze the IE, and the ability to plan and integrate IO activities in coordination with other joint operations, are critical competencies for the Joint Force.

[22] Department of Defense, *Strategy for Operations in the Information Environment*, 6.

All conventional military and Special Operations Forces must understand the requirements to shape pre-conflict environments in phase zero and how operations in the IE contribute to an overall strategic effort. Additionally, peer adversaries are unlikely in the near future to pursue open conflict with the U.S. so DoD leadership must understand how the USG and military must evolve to counter threats dynamically. The DoD must find ways to regain proactive dominance in the information environment as it relates to the battlefield. Information interlopes across all the instruments of national power, and it provides leverage for diplomatic, military, and economic efforts to achieve national security objectives. The author seeks to inform the evolution of the DoD's approach to Unified Action in future conflicts and implementation of the *DoD Strategy for Operations in the Information Environment*.

Assumptions

Given GEN Breedlove's statements about the U.S. ability to deal with Russia, one can assume that the U.S. is currently unprepared to mobilize and effectively synchronize the information instrument of national power across the USG in conjunction with the other instruments at the same level demonstrated by Russia. Russia and other adversary states have state-controlled media and the ability to influence domestic and international narratives, which is also unlikely to change.

Russia will continue to employ its Information Security Doctrine to achieve military and political objectives using NGW. Supporting this assumption is the fact that Russian President Vladimir Putin signed strategies and concepts from the new

Information Security Doctrine into Russian law.[23] Additionally, reports of Russian interference in Western democratic elections and demonstrated effectiveness of Russian information related capabilities employed in Ukraine further support this assumption.

While there was a shift in foreign policy under Dmitri Medvedev between 2008 and 2011 that leaned toward the West, Vladimir Putin reverted to previous anti-western foreign policy when he became president again in 2012.[24] Therefore, Russian foreign policy is unlikely to change given Putin's reelection in March 2018. Russia will employ NGW leveraging a whole-of-nation strategic and operational approach in current and future conflicts. Further, Russia will not curb this activity unless forced to cease by external entities, given the securitized nature of the state.

Scope

The author focused on Russia's smart power projection in Ukraine leading up to their 2014 incursion into Crimea, implications for the U.S. and NATO, and how the U.S. should respond as it refocuses its force to prepare for large-scale combat operations. Russian NGW, composed of irregular warfare and information warfare activities in Crimea and Donetsk (Donbas) are the geographic and operational boundaries of this analysis. This research explores the weaponization of social media to affect cultural and social change to support Russia's NGW strategy.

---

[23] Timothy L. Thomas, *Kremlin Kontrol: Russia's Political-Military Reality* (Fort Leavenworth, KS: Foreign Military Studies Office, 2017), 231.

[24] Andrei P. Tsygankov, "Foreign Policy and Relations with the United States," in *Putin's Russia: Past Imperfect, Future Uncertain,* ed. Stephen K. Wegren, 6th ed. (Lanham, MD: Rowman and Littlefield, 2016), 233.

With regard to U.S. military capability gaps, this study leveraged the capabilities-based assessment framework used in the Joint Capabilities Integration Development System process: Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P). The author determined after initial research to focus on doctrine, organization, and leadership education as areas in which some changes can significantly improve understanding of operations in the information environment across the DoD. Recommendations focused on improving the ability of the DoD to operate in the IE as part of a synchronized USG plan.

Limitations

The author only considered unclassified open source information for this thesis. Details about the Russo-Ukrainian War presented an issue of classification for a more in-depth understanding of Russian activities, Russian intentions and capabilities to inform conclusions about United States evolution. Also, possible intelligence oversight regulations limited the depth of analysis conducted by the investigator of aspects of social media use for propaganda and deception. Unfortunately, many valuable primary sources about Russian policy and activities in Ukraine are in Russian. The author relied on secondary sources or translated copies of Russian primary source documents.

Delimitations

This thesis will not delve into Russian activities outside of Ukraine and Crimea nor will it address the activities of the other primary adversaries of the U.S. which are

China, North Korea, Iran, and Violent Extremist Organizations.[25] The focus is within a single country-Ukraine-and Russian use of digital and social media and electronic warfare aspects of information warfare at the strategic, operational, and tactical levels of warfare. The allegations of Russian interference with the 2016 U.S. Presidential election will also not be part of in-depth analysis but rather provide some supporting background context. Additionally, this research will only focus on the information and military instruments of national power.

For the analysis of U.S. military capability gaps, the author only analyzed the doctrinal, organizational, and leadership education aspects of DOTMPLF-P. While policy, training and material aspects of this question remain important, other qualified researchers have either explored the technology aspect of information related capabilities including cyberspace operations, electronic warfare, and other special technical operations, or specific aspects of those IRCs are classified. Additionally, the author examined activities in the "gray zone" before open conflict erupted but did not discuss activities U.S. Special Operations Forces nor those of the Central Intelligence Agency and other agencies within the USG. Finally, the focus of analysis remained at the strategic and theater strategic level to mitigate the risk of collateral spillage.

Summary

The analysis of Russian NGW in Ukraine established a template for the successful employment of strategy, doctrine, and tactics in the IE. This research explored gaps in the DoD's ability to counter Russian operations within the IE and proposed mitigations to

[25] President of the United States, *National Security Strategy of the United States of America* (Washington, DC: The White House, 2017), 25.

support a synchronized USG approach to competing with Russia. The author framed the problem of countering Russian Gray Zone aggression by looking at Russian national and military strategic objectives and methodology, then narrowed the focus to operational and tactical level examination of activities in Ukraine.

The next chapter, "Literature Review" presents relevant literature to set the context and identify gaps for the analysis that is presented in Chapter 4, "Analysis." Chapter 3, "Methodology" details the mixed methodology employed to conduct the research and explains the analytical framework that shaped chapter 4. From there, chapter 5 presents conclusions and recommendations for the DoD to adopt in the areas of doctrine, organization, and leadership education.

The research focused on Russia because the author assessed Russia as the greatest military threat in the IE based off evidence presented in the 2017 National Defense Strategy. The U.S. must compete in the IE with Russia now to influence at-risk or moderate audiences from becoming victims of Russian dis-information and disruption.

Competition with Russia in the IE should focus on building an integrated whole-of-society approach if it is to be successful. Based on delimitations, the author focused specifically on the military instrument of national power and the DoD's ability to operate in the IE as a step toward building a future unified approach. The last aspect to consider is the need not only for a whole-of-government approach developed by the U.S. but the inclusion of allies and partners in a strategic initiative in line with their national caveats and abilities.

CHAPTER 2

LITERATURE REVIEW

> Russia is never as strong as she looks, but Russia is never as weak as she looks.
>
> — Russian Proverb

Introduction

The author intends to define the DoD's critical capabilities, illustrate gaps in the planned execution of these capabilities, and propose mitigations to compete with and defeat adversaries in the IE. Academia and the military are replete with scholarly works on the current Russo-Ukrainian War and Russian international relations, but literature is sparse regarding unclassified IO doctrine, organization, and leadership education. The first section of this research provides context on Russian strategic and regional objectives and how it leverages the information instrument of national power to achieve progress towards those national objectives specifically in Ukraine. Included in this section is how Russia leveraged digital and social media for use in social change through active measures as part of its NGW strategy. Finally, the DoD's abilities to conduct operations within the information environment as an aspect of the military instrument of national power comprises the last section of the literature review.

Russian NGW and Information Warfare

To address recommendations for operations in IE, one must first understand how the adversary thinks about the problem. While there is a plethora of published information on this topic, two authors have current works in these areas that stand out:

Timothy Thomas and Marcel Van Herpen. This section of the literature review will focus on their works and then transition to a refined look at the strategy employed in the IE to support operations in Ukraine.

Thomas' works *Russia: Military Strategy*, *Kremlin Kontrol*, and *Recasting the Red Star* thoroughly describe Russian policy and strategy documents, define terms, and provide background and context to the Russian overall and military strategies. As a former Foreign Area Officer specializing in Russian Studies, he drew upon his years of experience and researched publicly available information and unclassified documents while serving at the Foreign Military Studies Office at Fort Leavenworth, Kansas. Thomas is one of the foremost experts on Russian use of Information Warfare (IW). Thomas highlights that "the ultimate aim of Russia's media disinformation machine is to destabilize the West."[26]

Given that NGW is a whole-of-nation strategy, there are multiple facets to it including information warfare, traditional warfare, political warfare, and economic warfare. Russia leverages these military and non-military activities in a synchronized manner to execute the strategy. The characteristics of NGW led the U.S. to coin various terms to describe Russian strategy such as "hybrid warfare" and NGW. In their study of the Russo-Ukrainian War, army officers Amos Fox and Andrew Rossow ascribe to Robert Leonhard's description of hybrid warfare in their Land Warfare paper: [27]

---

[26] Thomas, *Kremlin Kontrol*, 54.

[27] Amos Fox and Andrew Rossow, *Making Sense of Russian Hybrid Warfare: A Brief Assessment of the Russo Ukrainian War* (Arlington, VA: Institute of Land Warfare, 2017), 3.

> Hybrid operations are characterized by the undeclared action that combines conventional and unconventional military operations, while coupling military and nonmilitary actions in an environment in which the distance between strategy and tactics has been significantly reduced and where information is critically important.

However, Thomas argues that the term "hybrid warfare" is a Western appellation and that according to Russian doctrine, their strategy is simply named "new-type warfare." In this thesis, the author refers to this concept as NGW. Figure 1 depicts a recreation of Thomas' translation of a Russian graphic representation of NGW which could serve as a planning map for Russian strategy and operations at the onset of the current Russo-Ukrainian war. It outlines an approach with three lines of effort. First, Russia increases diplomatic strategic communication and propaganda efforts to disseminate the Russian narrative and themes to regional and global audiences. This line of effort includes leveraging political and economic pressure and weaponizing information to psychologically impact targeted audiences and decision makers of the enemy state. Second, the Russian military shifts to executing traditional warfare activities integrating weapons and information capabilities to achieve kinetic and non-kinetic effects in support of the plan. The third line of effort consists of executing operations to simultaneously seize key territory or infrastructure and the destruction of enemy forces in depth to gain control of the enemy state. This part is reminiscent of Tukhachevsky's concept of Deep Battle with modern applications of technology and incorporation of what the U.S. would call the cyberspace operational domain.

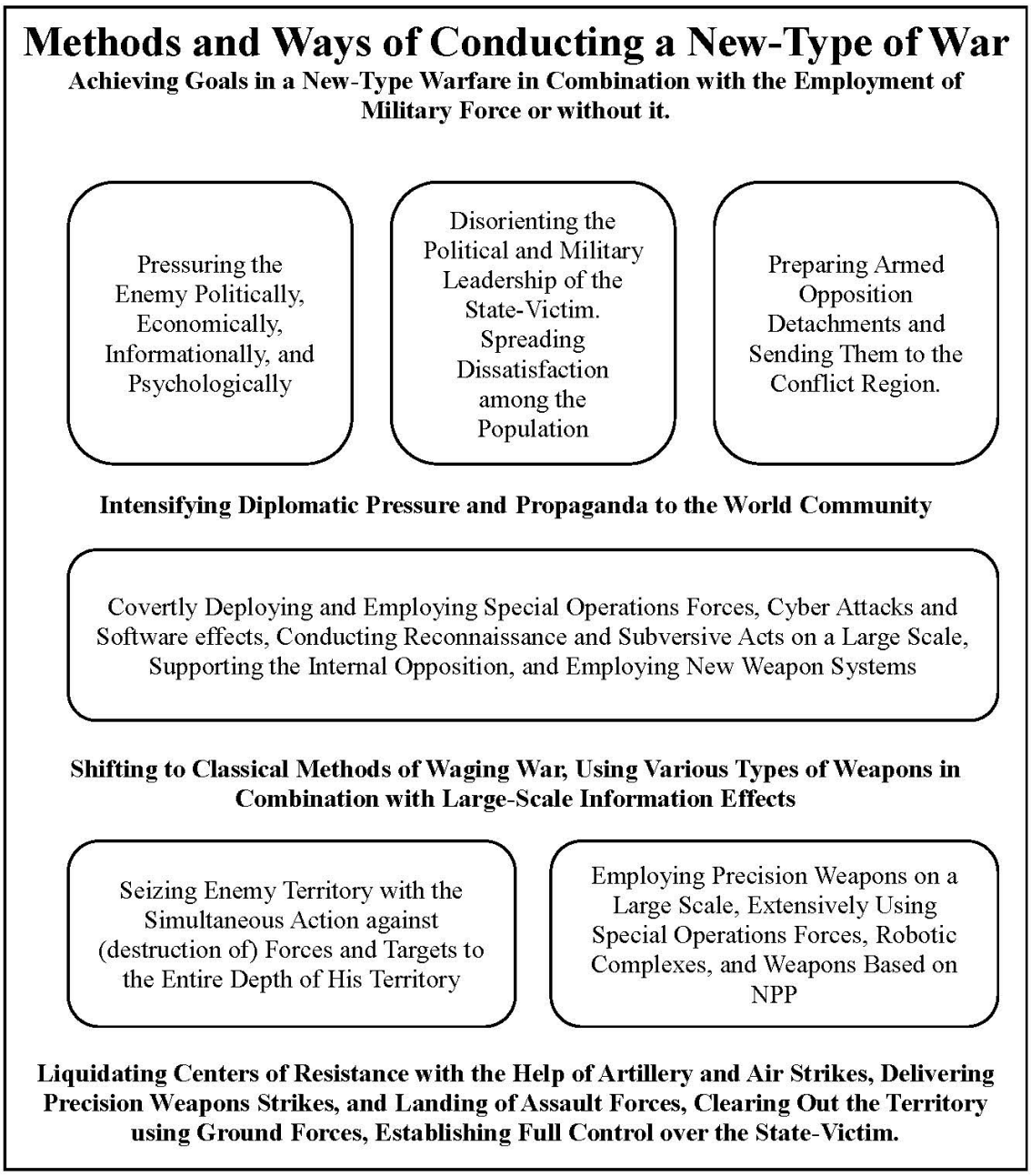


Figure 1. Methods and Ways of Conducting a New-Type of War

Source: Recreated by author from Timothy Thomas, *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics* (Fort Leavenworth, KS: Foreign Military Studies Office, 2015), 106.

At the tactical level in large-scale combat, Russia leverages information capabilities to enable maneuver and fires. "Deception, electronic warfare, and strikes against command and communications—are intended to disrupt adversaries and slow their ability to respond to developments on the battlefield."[28]

Figure 2 depicts a Russian phasing model for NGW which is a derivative of the model Charles Bartles' translated from Russian primary documents and published in *Military Review*.

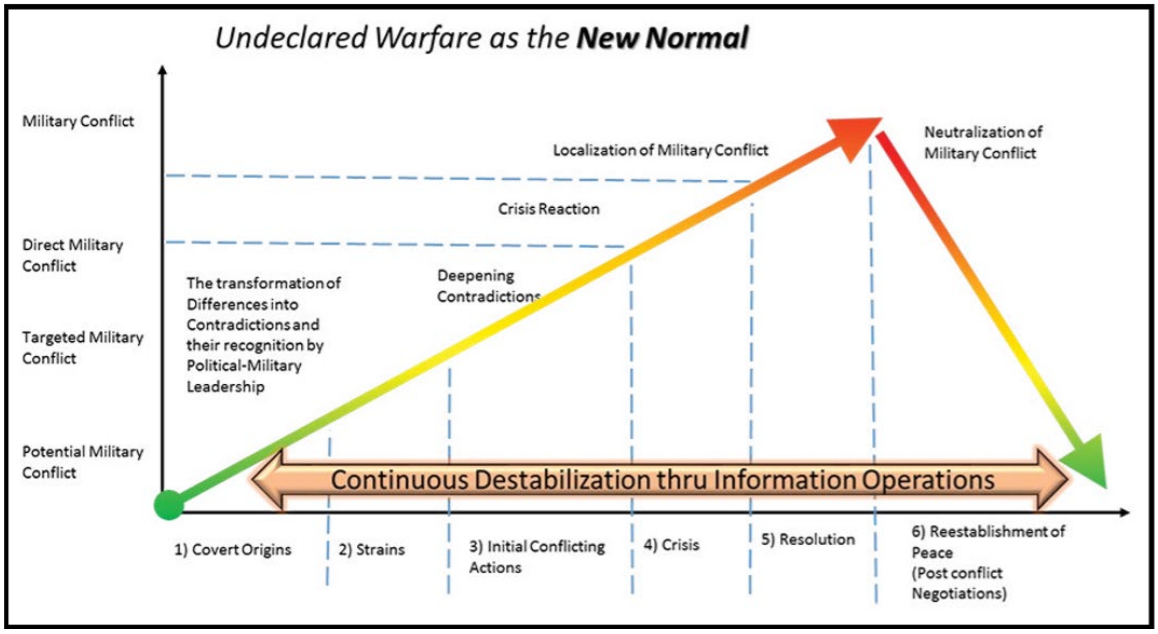


Figure 2. (U) Russian Phases of Conflict in New Generation Warfare

Source: Asymmetric Warfare Group, CALL Handbook No. 17-09, *Russian New Generation Warfare* Version 2.1 (U//FOUO) (Fort Meade, MD: Asymmetric Warfare Group, April 2017), 19. The CALL Handbook No. 17-09 is Unclassified//For Official Use Only, but this particular figure is unclassified and authorized for unlimited distribution.

[28] Scott Boston and Dara Massicot. *The Russian Way of Warfare: A Primer* (Santa Monica, CA: RAND Corporation, 2017), 9.

In figure 3, the author presented a recreated figure that consolidates multiple translations of the Russian strategic approach, including Bartles'. Figure 3 modeled the phases of Russian NGW and underneath the phasing model, the figure depicts the military and non-military activity executed within the various instruments of national power in relation to the phases. Highlighted with a red box, the author calls attention to the fact that the Russians view their information conflict (warfare) doctrine as activity that occurs throughout the spectrum of conflict. The figure encompasses the whole-of-nation approach and shows both military and non-military means employed to achieve strategic objectives. Also significant is that the "Conduct information warfare/conflict" box straddles the military and non-military bands of activity within the NGW construct, demonstrating that Russia might view the information instrument of national power as the most significant, albeit not decisive.

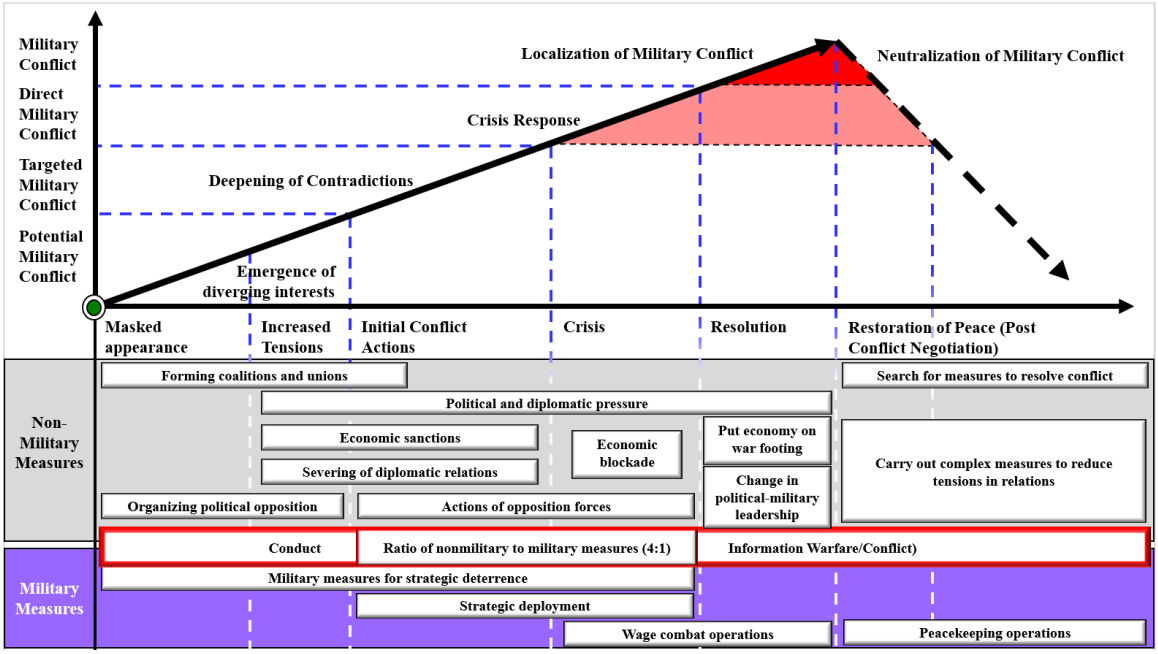


Figure 3. Russia's Whole-of-Nation Strategic and Operational Approach in NGW (The Gerasimov Chart)

Source: Created by author from multiple translations of Russian source documents.

Specific to the information instrument of national power is Russian IW, defined by V.K. Novikov and S.V. Golubchikov as:

> an extension of a country's politics that consists of purposeful, comprehensive, and methodical informational impacts against foreign information targets in order to achieve political, economic, territorial, national, religious and other goals with minimal loss of life and physical damage and without occupation of foreign soil while protecting its own information sources.[29]

To successfully conduct NGW, a state must synchronize efforts across the instruments of national power in pursuit of strategic objectives. In his *Military Review* article, "Expanding Tolstoy and Shrinking Dostoyevsky," Scott Harr identifies that Russian employment of a whole-of-nation integrated approach to information warfare as

[29] В.К. Новиков, С.В. Голубчиков, 10-16.

a strategy. He also addresses Russia's lack of bureaucratic constraints in their execution of information campaigns. Specifically, he highlights an imbalance between Russian and U.S. information warfare policy.[30]

However, he does not account for what joint doctrine calls "phase 0" information operations, which is also known as the gray zone, which are pre-conflict activities. Specific to this case study on Russian IW efforts in Ukraine, Harr's omission of gray zone consideration detracts slightly from the value of his piece to this specific research, but still provides insight into overall Russian IW.

Van Herpen argues that three components, mimetis, rollback, and invention comprise the new Russian "soft-power offensive." Declaring invention the most important, he defines it as, "a strategy to invent new soft-power strategies, making ample use of the possibilities offered by the open Western societies."[31] This soft-power offensive and the idea of "soft power in a velvet glove" similarly describes what the National Endowment for Democracy's Christopher Walker and Jessica Ludwig coined as "sharp power."[32] These analyses continued to demonstrate that Russian aggression is problematic and will be deceptive and coercive.

---

[30] Scott Harr, "Expanding Tolstoy and Shrinking Dostoyevsky," *Military Review* (September-October 2017): 45.

[31] Marcel H. Van Herpen, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (Lantham, MD: Rowman and Littlefield, 2016), 34.

[32] Christopher Walker and Jessica Ludwig, "The Meaning of Sharp Power: How Authoritarian States Project Influence," *Foreign Affairs,* 16 November 2017, accessed 26 April, 2018, https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power.

In the *2018 National Defense Strategy of the United States of America*, Secretary Mattis expanded the language from his guidance memorandum to the DoD in his description of the Russian threat that essentially matches strategy for NGW:

> Russia seeks veto authority over nations on its periphery in terms of their governmental, economic, and diplomatic decisions, to shatter the North Atlantic Treaty Organization and change European and Middle East security and economic structures to its favor. The use of emerging technologies to discredit and subvert democratic processes in Georgia, Crimea, and eastern Ukraine is concern enough, but when coupled with its expanding and modernizing nuclear arsenal the challenge is clear.[33]

From 2013 to 2017, Russia's foreign policy strategy towards Ukraine involved a whole of nation approach to achieve national objectives. The information instrument of national power was the core of its apparatus, given that the other instruments derived leverage from information. Russia revived anti-western policies of the United Soviet Socialist Republic and challenging NATO on its frontier as evident from its activities in Ukraine. Russia adopted Soviet-era policy mechanisms to their current foreign policy. One of these mechanisms was active measures, a Soviet-era term used to describe information, psychological, or political means conducted to advance Soviet foreign policy goals and extend influence throughout the world.[34]

The Brookings Institute published a study by Alina Polykova and Spencer Boyer on political warfare in 2018 that outlined the goals and methods of Russia's disinformation campaigns. It specified that Russia's goals are:

---

[33] Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, 2.

[34] Scott Marler, "Russian Weaponization of Information and Influence in the Baltic States" (Master's Thesis, Command and General Staff College, Fort Leavenworth, KS, 2017), 69.

- Undermine the Western political narrative and trans-Atlantic institutions;
- Sow discord and divisions with countries
- Blur the line between fact and fiction.[35]

The methods Polykova and Boyer identified were: full-spectrum dissemination and amplification of misleading, false, and divisive content; deployment of computational propaganda; identification of societal vulnerabilities.[36]

A second mechanism employed by Russia is maskirovka, which leverages deception. Thomas highlights how the 2007 Russian Military Encyclopedic Dictionary defines "maskirovka":

> A complex of undertakings aimed at concealing troops (forces) and assets from the enemy and deceiving it regarding the presence, disposition make-up, state, actions, and intentions of troops (forces), as well as the plans of the command; a type of battle (operational) support.[37]

Another mechanism Russia used is reflexive control, which Thomas defined as a "means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[38] Russia executed reflexive control by employing a combination of military and

---

[35] Alina Polykova and Spencer P. Boyer, *The Future of Political Warfare: Russia, The West, and the Coming of Age of Global Digital Competition* (Washington, DC: Brookings Institute, 2018), 4.

[36] Ibid.

[37] Timothy Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness* (Fort Leavenworth, KS: Foreign Military Studies Office, 2011), 386.

[38] Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17 (2004): 237-256. DOI: 10.1080/ 13518040490450529.

non-military measures categorized as Information/Technology and Information/Psychological.

For example, Thomas describes an episode in Ukraine where Russia invited Organization for Security and Cooperation in Europe inspectors to their location as the Russians initiate a bombardment of Ukrainian forces, which the Ukrainians must retaliate in self-defense. The Russians timed it so that the inspectors arrive to record the Ukrainian retaliation against the Russian positions. Thus, the inspectors only captured half the story. By manufacturing "realities" like this, the Russians capitalize on the event to present half-truths and disinformation to shape perceptions against the West and the government in Kiev. This mechanism fits in well with how the Soviet Union--and now Russia--execute deception and leverage "sharp power."

Van Herpen argues that Russia twisted what Nye coined as soft power into something Westerners would view as hard power. Van Herpen calls this a new Russian "soft-power offensive." Declaring invention as the most important component of this "soft-power offensive," he defines it as, "a strategy to invent new soft-power strategies, making ample use of the possibilities offered by the open Western societies."[39] This soft-power offensive and the idea of "soft power in a velvet glove" similarly describes what Walker and Ludwig coined as "sharp power." Nye explains their concept of sharp power as that, "which 'pierces, penetrates, or perforates the political and information environments in the targeted countries,' with 'soft power,' which harnesses the allure of

[39] Van Herpen, *Putin's Propaganda Machine*, 34.

culture and values to enhance a country's strength."[40] Nye further explains that "sharp power [is] the deceptive use of information for hostile purposes, [and] is a type of hard power."[41]

Dr. Jolanta Darczewska, head of the Department for Internal Security in Eastern Europe at Osrodek Studiow Wschodnich and expert on security in post-Soviet states, published multiple papers of Russian information warfare. She leveraged many Russian strategy documents as her primary sources for research and translated the military definition of information war as:

> the confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilize the state and society, as well as the coercion of the state to take decisions for the benefit of the opposing force.[42]

While this definition differs slightly from Novikov and Golubchikov's, the core principles remain: disrupt systems and decision-making, undermine the social values, and destabilize the adversary state.

---

[40] Joseph S. Nye Jr., "How Sharp Power Threatens Soft Power: The Right and Wrong Ways to Respond to Authoritarian Influence," *Foreign Affairs,* 24 January, 2018, accessed 19 February, 2018, https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power?cid=int-fls&pgtype=hpg&utm_source=Sailthru&utm_medium=email&utm_campaign=ebb%2001.25.2018&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief.

[41] Ibid.

[42] Jolanta Darczewska, "Russia's Armed Forces on the Information War Front: Strategic Documents" (OSW Studies, Warsaw, June 2016), 47.

Russian Employment of NGW in Ukraine

Literature abounds on the Russo-Ukrainian War regarding Russian gray zone activities, IW, and leverage of social media to set conditions for military activity. Many scholarly works exist on political warfare, active measures, influence via social media, and tactical employment of information capabilities. These various academic works address many aspects of information activities of NGW in Ukraine at strategic, operational, and tactical levels.

At the strategic level, Russia exerted economic and political pressure on Ukrainian President Yanukovych which led to the crisis in 2014. Echoing Thomas's conclusions, Leonhard concludes that the Russian efforts in Ukraine:

> [Were] [d]riven by a desire to roll back Western encroachment into the Russian sphere of influence, the current generation of Russian leaders has crafted a multidisciplinary art and science of unconventional warfare. Capitalizing on deception, psychological manipulation, and domination of the information domain, their approach represents a notable threat to Western security. The new forms of Russian unconventional warfare challenge the structure of the NATO Charter, because they obviate the appearance of "armed invasion."[43]

The author also sought to understand Russian use of social media for the proliferation of propaganda as part of political warfare and setting conditions for the annexation of Crimea and the incursion into Eastern Ukraine. Digital and social media during the Information Age exponentially expanded access to and the dissemination of information. A digital camera, computer, and internet connection allow anyone to send their message out to the connected world. The introduction of smartphones combined all

[43] U.S. Army Special Operation Command, *Little Green Men: a primer on Modern Russian Unconventional Warfare Ukraine 2013-2014* (Fort Bragg, NC: Special Operations Command, 2016), 3.

three of these necessary components into one device, placing a small computer in the hands of any user. These devices provide the perfect weapons of information warfare.

The RAND Corporation published a study in 2018 on Russia's use of social media in Europe. Entitled *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, this study reviewed the 40 most relevant articles found through keyword searches on Google and Google Scholar to determine the themes and methodology used by Russia in Ukraine and other European states. Of the study's objectives, two are relevant to this paper's primary and secondary research questions. The RAND researchers sought to understand the nature of Russia's social media propaganda and they sought to understand challenges for Western policy-makers to mitigate Russian influence in the region.[44]

With regard to use and impact of social media for propaganda in Ukraine, Russia utilized a mixture of traditional and social media platforms of varying levels of attribution in a form of active measures conducted through social media. According to the RAND study, the employment of trolls and bots were a significant part of the Russian social media propaganda campaign. Russia combined the propaganda effort with irregular warfare elements of military special operations and intelligence personnel to generate a Ukrainian pro-Russian force of surrogates and proxies capable of seizing and holding terrain. Liane Rothenberger, a researcher who specializes in terrorism and media, also highlights the value of social media use:

---

[44] Todd C. Helmus et. al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: RAND Corporation, 2018), iii.

> Social media offer the possibility of reaching a wide audience in all parts of the world, and of networking and establishing contacts—an essential part of PR efforts. They can play a crucial role for the groups' self-organization as they offer anonymous interchange and volatility. The terrorists can also use it as a propaganda tool to distribute their ideas of political change.[45]

Then-Major Nathanael Burnore, an Army IO officer, wrote in 2013 about U.S. military experience with enabling Unconventional Warfare with social media campaigns, "for [unconventional warfare] is that there exists an increasing need to bring multiple groups together (as with the Northern Alliance in Afghanistan) to accomplish an objective. In creating this fusion, social media is a powerful agent."[46]

At the tactical level, the Russian Electronic Warfare (EW) capabilities provided a significant advantage to pro-Russian Ukrainian separatists. Igor Sutyagin and Justin Bronk, two research fellows at the Royal United Services Institute highlight:

> A triple role is envisaged for EW units in the Russian land forces. The first is the disruption of enemy command-and-control networks and communications channels. The second is countering an adversary's intelligence, reconnaissance and surveillance activities with active and/or passive radar-based techniques. The third is defending friendly forces against enemy artillery, missile and air-dropped munitions.[47]

---

[45] Liane Rothenberger, "Terrorist Groups: Using Internet and Social Media for Disseminating Ideas," *Romanian Journal of Communication and Public Relations* 3 (March 2012): 10.

[46] Nathanael Burnore, "Social Media Application for Unconventional Warfare" (Master's Thesis, Command and General Staff College, Fort Leavenworth, KS, 2013), 59.

[47] Igor Sutyagin and Justin Bronk, "Russia's New Ground Forces: Capabilities, Limitations and Implications for International Security" (Whitehall paper, RUSI, 2017), 81.

The DoD and the Information Environment

In this section, the author focused on DoD policy, joint and service doctrine, and scholarly writing regarding the organization and education of IO as it relates to military officer education. Reinforcing a reason for the misunderstanding of IO, Paul Scharre proffers that one of the three main obstacles to adaptation to future warfare is "cultural resistance within elements of the military to new paradigms of warfighting."[48] While a plethora of published literature exists on the material aspects of IO, specifically with cyberspace operations and electronic warfare, there is limited published information s on the education of IO in the DoD. The majority of published material that does exist is generally is more than ten years old with some notable exceptions from IO officers Lieutenant Colonel Christopher Lowe, Colonel Maxwell Thibodaux, and Colonel Mark Vertuli.

Before reviewing doctrinal definitions, let's define the dimension of the IE and explain how IO achieves effects in the environment and how gaps and misunderstanding can exist due to its complexity. Physical, informational, and cognitive dimensions comprise the IE. First, the physical dimension consists of the tangible things in the real-world like "[command and control (C2)] systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects."[49] Some things included in this dimension of the IE are humans, end-user devices like cellular phones

[48] Paul Scharre, "Readying the U.S. Military for Future Warfare" (Testimony before the House Armed Services Committee, 30 January 2018), accessed 23 March 2018, https://www.cnas.org/publications/congressional-testimony/paul-scharre-testimony-before-hasc-2.

[49] Joint Chiefs of Staff, JP 3-13, *Information Operations*, I-2.

and laptops, computer servers, radio broadcast towers, transmitters and receivers, and Command and Control (C2) locations. Next, the informational dimension is the unseen realm of "where and how information is collected, processed, stored, disseminated, and protected."[50] It is the command and control of entities and milieu of commander's intent. Finally, the cognitive dimension:

> encompasses the minds of those who transmit, receive, and . . . act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making . . . this dimension constitutes the most important component of the [IE].[51]

To provide context to current doctrine, the author drew upon various policy documents and doctrine manuals to contextualize current doctrinal issues and the proffered recommendations in chapter 5. As previously noted, JP 1-02 *Dictionary of Military and Associated Terms* and JP 3-13 *Information Operations* define IO as:

> The integrated employment, during military operations, of information-related capabilities [IRCs], in concert with other lines of operation, to influence, disrupt, corrupt, or usurp the decisionmaking of adversaries, or potential adversaries, while protecting our own.[52]

The Marine Corps amplifies the JP 1-02 definition of information operations:

> Information Operations is the integration, coordination, and synchronization of all actions taken in the information environment to affect a target audience's behavior in order to create an operational advantage for the commander.[53]

---

[50] Ibid., I-3.

[51] Ibid.

[52] Joint Chiefs of Staff, Joint Publication (JP) 1-02, *Dictionary of Military and Associated Terms* (Washington, DC: Government Printing Office, 2010), 110; and Joint Chiefs of Staff, JP 3-13, *Information Operations*, ix.

[53] U.S. Marine Corps, MCRP 1-10.2, *Marine Corps Supplement to the DOD Dictionary of Military and Associated Terms* (Washington, DC: Government Printing Office, August 2013), II-32.

Joint doctrine defines IRC and the application framework of them:

> IRCs are the tools, techniques, or activities that affect any of the three dimensions of the information environment. The joint force (means) employs IRCs (ways) to affect the information provided to or disseminated from the target audience (TA) in the physical and informational dimensions of the information environment to affect decision making.[54]

Army doctrine further amplifies discussion of IRCs:

> IRCs are those capabilities that generate effects in and through the information environment, but these effects are almost always accomplished in combination with other information-related capabilities. Only through their effective synchronization can commanders gain a decisive advantage over adversaries, threats, and enemies in the information environment. While capabilities such as military information support operations, combat camera, military deception, operations security and cyberspace operations are readily considered information-related, commanders consider any capability an IRC that is employed to create effects and operationally-desirable conditions within a dimension of the information environment.[55]

One seminal scholarly work that accounts for the perceived disjointedness of military IO is then-Major Christopher Lowe's, "From 'Battle' to 'Battle of Ideas': The Meaning and Misunderstanding of Information Operations." Lowe explored the genesis of IO by reviewing the emergence of Command, Control, and Communication Countermeasures and Command and Control Warfare (C2W), the precursors to IO, as responses to Soviet doctrine. Lowe also explains the discrepancy of the technical side of IO and the wars of narratives, messages, and ideas. He posits that after the Military Operations Other Than War era of the 1990s, specifically the Balkan conflict when the Task Force staff assimilated the psychological operations (PSYOP) in with the IO staff and thus began the confusion about what IO is in practice. He highlights the functional

---

[54] Joint Chiefs of Staff, JP 3-13, *Information Operations*, x.

[55] Department of the Army, Field Manual 3-13, *Information Operations* (Washington, DC: Government Printing Office, 2016), vi.

design of IO began as a response to the 1974 Soviet doctrine of Radio-electronic Combat. Lowe quoted the definition and purpose from previous studies as:

> an 'integrated system' that combined 'signal intelligence, direction finding, intensive jamming, deception, and suppressive fires to attack enemy organizations and systems throughout their means of control'. . . to limit, delay, or nullify the enemy's use of his command and control systems, while protecting one's own.[56]

One scholarly work on IO organizational structure is by COL Maxwell Thibodaux. He wrote in 2013 on Army restructuring for information warfare by contrasting proposed models with Naval and Air Force models. His proposed models center around an Army Information Corps as a career grouping of branches. He does not focus on joint organizations or the DoD writ-large.

While the need for tactical deception will be critical in the event of large-scale combat operations, the land forces are not proficient in it.[57] Historically, there were tactical units that supported deception at the tactical, operational and strategic levels. The Army stood up the 23rd Special Troops, an O-6 level command during World War II. Four main subordinate units comprised the 23rd Special Troops: a signal deception company, an engineer camouflage battalion, a combat engineer company, and a sonic deception company.[58] These units enabled 20 operations in the European Theater of Operation including the invasion at Normandy by creating fake units with decoys, fake

---

[56] Christopher Lowe, "From 'Battle' to 'Battle of Ideas': The Meaning and Misunderstanding of Information Operations" (Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2010), 45.

[57] Mark D. Vertuli, "A Myth Retold: The Army's MILDEC Program in the 21st Century," *IO Sphere* (Fall 2015): 19.

[58] Johnathan Gawne, *Ghosts of the ETO: American Tactical Deception Units in the European Theater of Operations 1944-1945* (Havertown, PA: CASEMATE, 2002), 305.

unit patches and unit vehicle identification numbers, and creating radio traffic for units that did not exist for German intelligence assets to observe.

Critical to success in deception is detailed information and intelligence. In the Information Age, overwhelming information is readily available to the public in open source media rather than being hidden as classified intelligence requiring specialized activities to collect. Robert Steele, one of the foremost proponents of open source intelligence, argues in 2006 that, "[i]n the Age of Information, the primary source of national power is information that has been converted into actionable intelligence or usable knowledge."[59] Steele focuses on the national level but touches on some key points about information. Specifically, he proffers that IO has three elements: strategic communication, which he calls "the message;" open source intelligence, which he calls "the reality;" and joint information operations centers, which he calls "the technology."[60] Steele also states,

> IO, if carried out by DoD in the enlightened manner that is potentially possible, has the possibility of revolutionizing governance by revolutionizing what government can know, how it knows it, how it decides, and how it communicates both its decision and supporting information. Modern IO is the first step toward revolutionary wealth.[61]

Steele's monograph deftly connects the three elements of IO and demonstrates a good understanding of operations in the IE from a whole-of-government approach that can easily translate to military professionals.

---

[59] Robert David Steele, "Information Operations: Putting the "I"" back in DIME" (Report, Strategic Studies Institute, Carlisle, PA, 2006), 1.

[60] Ibid., 6.

[61] Ibid., 23.

The other side to open source intelligence is the ability to project information into the open source media to achieve wider influence. A significant venue for influence is digital and social media. IO officer MAJ Scott Marler posits in his thesis on Russian influence in the Baltic states that:

> The best strategy to combat Russian propaganda is not Western propaganda; instead, the US and its allies must contest Russian themes in open source media according to Western values, and dedicated assimilation of minorities in accordance with Western liberal values.[62]

Former Assistant Secretary of Defense for Special Operations/ Low-Intensity Conflict and director of the Global Engagement Center (GEC) Michael D. Lumpkin testified before the House Armed Services Committee about the challenges in leveraging digital and social media to counter adversary propaganda efforts:

> social media environment and the media environment writ large is changing so rapidly, what we find ourselves frequently doing is putting 2-year-old tools into the workforce because that is how long it takes to get approvals to use them in many cases.[63]

Summary

In this chapter, the author presented background information to define IO within the IE by highlighting Russian NGW in Ukraine and areas in which the DoD is unable to counter this type of aggression effectively. Given the contradictions and ambiguity in doctrine pertaining to IO and the datedness or sparseness of literature on IO organizations

---

[62] Scott Marler, "Russian Weaponization of Information and Influence in the Baltic States," 62.

[63] U.S. Congress, House, *Crafting an Information Warfare and Counter-Propaganda Strategy for the Emerging Security Environment* (Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services, 115th Cong., 1st sess., 15 March 2017), 25.

and education, there are certainly literature gaps and areas in which the joint force can improve to compete with Russia in the IE.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

The author employed mixed methods research design methodology to answer the primary and secondary research questions: a qualitative case study on Russian strategy and activities in Crimea and Eastern Ukraine from 2013 to 2017 through compilation and analysis of scholarly research. The author attained additional information on the Russo-Ukrainian War from semi-structured interviews with United States European Command personnel into the analysis of Russian activities. Additionally, the author conducted interviews with IO personnel to gain perspective on current information operations doctrine and decision making affecting IO. Additionally, the author conducted a partial DOTMLPF-P review of current and historical joint and service doctrine, the DoD IO enterprise organizational structure, and Professional Military Education (PME) curricula.

Within the case study, the author reviewed Russian strategic objectives and its employment of capabilities in support of NGW to demonstrate how Russia employed information to support military and national objectives. For qualitative and quantitative analysis of DoD capabilities, the author conducted interviews, compiled and analyzed documents and survey data on U.S. doctrine, organization, leadership education relating to information operations and operations in the information environment comprised the documentation review to identify gaps in U.S. capability to respond to Russian threats. Specific to doctrine review, the author sought to identify inconsistencies in terminology and contradictions across the service and joint manuals to best understanding why the joint force has a fundamental misunderstanding of IO and to proffer recommendations.

Capabilities-Based Assessment

The DoD's force management process includes the Joint Capabilities Integration Development System. This process identifies capability gaps by conducting Capabilities-Based Assessments. The author focused on three elements of DOTMLPF-P analysis that included doctrine, organization, and leadership education elements to maintain a strategic focus. Despite that a comprehensive Capabilities-Based Assessment has not been conducted, this thesis does not aspire to conduct a full Capabilities-Based Assessment in order to adhere to the limited research scope.

To analyze joint and service component doctrine, the author traced IO definitions, terminology, and integration of IO back through 25 years of doctrine manuals. This method made inconsistencies, contradictions, and gaps evident and shaped recommendations. These recommendations seek to improve servicemembers' ability to enhance understanding of IO and the IE through the self-development pillar of leader development.

To analyze organizational structures, the author reviewed current IO, joint, and service organizational structures and interviewed various IO professionals that support the joint force to identify if command and control relationships, stove-piping, and service-biases might contribute to the problem of misunderstanding IO and the IE due to asynchronous efforts and lack of communication.

To analyze leadership education, the author reviewed PME programs of instructions to compare the number of hours of instruction on IO and interviewed faculty at the U.S. Army Command and General Staff College (CGSC), the Army Force Modernization Proponent Office, responsible for conducting the IO qualification course,

and 1st IOC. Additionally, the online survey provided qualitative and quantitative data on the integration of formal IO instruction at CGSC. By triangulating data generated from this mixed method, the author compiled data from multiple vectors to develop a more holistic synthesized set of conclusions and recommendations.

Interviews

During this research, the author conducted semi-structured interviews with personnel from United States European Command, 1st Information Operations Command (1st IOC), IO and doctrine professionals. These interviews informed the analysis with context on Russian activities in Ukraine, Information Operations, and DoD decision making about DoD evolution of IO capabilities. Interviewees were subject matter experts in their fields who had invaluable insight relevant to this research based on years of experience and academic study. The interviewees gave informed consent to attribute their remarks and had the opportunity to amend their statements before finalization of this thesis. They also were informed that participation did not equate to any reward or compensation.

Survey

The purpose of the online survey was to generate new data on the effectiveness of IO instruction in PME among DoD servicemembers. These results generated a qualitative perspective on the perception of IO and IO professionals from the future organizational and strategic leaders of the Armed Forces. The online structured survey provided qualitative and quantitative data using the Likert Scale, multiple choice responses, and free response answers to questions about doctrine, organization, and PME curriculum.

The Likert scale is a five-degree qualitative scale that ranges from “Strongly Agree” to “Strongly Disagree.” Respondents had the opportunity to provide additional information to support positive and negative responses.

International officers, interagency personnel, and a U.S. Coast Guard student were excluded from the sample group because the author focused on DoD military professionals to generate data that will provide insight into recommendations for U.S. military reform. The sample group began with 100 students who received the invitation to participate in the survey, with a 12 percent response rate. Survey participants were in-residence U.S. Army CGSC students across the DoD services. The voluntary survey remained confidential and issued to the student population by CGSC personnel. Risk was mitigated to ensure the identifiable information of the participants remained secure.

The administrative data collected at the beginning of the survey instrument provided context to facilitate qualitative analysis of the responses to generate thorough synthesis beyond simple qualitative statistics. Requested data provided explanations for outliers and trends in the survey results attributed to previous experience within their service or branch. Participants were not obligated to provide data to complete the survey. Information requested was the participants’ service, basic branch, and functional area and the number of years of IO experience. Also requested was: years of experience at the tactical level, defined as brigade and service-equivalents and below; operational level, defined as division through field army and service equivalents; and strategic level, defined as combatant command and higher, to include interagency positions.

Administrative data served as the context for analysis and identification of possible trends amongst the services and branches, but the data was not used to present

stratified data of survey responses. The author only presented the numbers of each type of response for the Likert Scale and multiple-choice questions in chapter 4. The instrument did not collect any other data as it could be collated and reveal personally identifiable information that would violate the intent of participant anonymity. Further, the author redacted any free responses to the survey that could potentially lead to deductive identification of the respondent from formal analysis.

Chapter 4, "Analysis," presents survey data in tables depicting the Likert scale responses broken down by raw numbers of respondents, the multiple-choice responses by percentage-highlighting the correct responses, and the open-ended responses were only used to address trends or reinforce assertions, as long as doing so did not increase risk to the participant's confidentiality. Due to a small return rate of the survey instrument, the generated data would not be valuable as discrete evidence to support the author's assertions. However, the triangulation of the survey data, interviews, and document reviews still support a stronger argument, as a whole.

Protections

Protection of participants was paramount during research involving interaction with personnel. Before execution of interviews and the online survey, an Institutional Review Board reviewed the research instruments to ensure that the risk to subjects was mitigated and that the instruments were both valid and would contribute to the research. The author gained documented informed consent from interviewees and notified them that their responses would remain secure and remarks attributed as they desired. All interviewees had the opportunity to read the transcripts of the interviews to add, edit, or redact content and review the final draft of this research to issue final consent to include

and attribute their responses. If an interviewee did not want a particular response attributed, the investigator determined whether the information was critical to the research. If the information was critical, the investigator presented the information in a manner that did not identify the interviewee, referencing a generic job title or "senior official," for example. If the information was not critical, the investigator sought other sources for the information or removed it from the thesis. Each interviewee had the option to withdraw consent at any time before publication. Survey respondents issued consent by their participation in the survey.

For interviews, the investigator informed the interviewee of the research purpose and the steps taken to protect their confidentiality to gain signatures on the consent form. The author transcribed audio recordings obtained with permission from the interviewees. Upon completion of transcription, the investigator destroyed the audio recordings to mitigate additional risk to the participant's confidentiality when desired.

For surveys, the only administrative data collected was the participant's branch of service, career field or control branch, and functional area, if applicable. Additional information included the number of years each participant served at the tactical, operational, and strategic levels, as well as previous experience with IO. The instrument collected this information to inform a better qualitative analysis of the newly generated data. No party collected additional demographic information from the participants during this research. The author waived documented informed consent to add an additional layer of protection to participants as the signed consent forms would be the only identifiable link from the participants to the survey. Instead, the participants issued their consent as part of their participation in the online survey by completing a two-click consent

procedure after reading the purpose of the study and explaining the protection of their personally identifiable information.

Summary

The mixed methods approach to this research using a case study and qualitative analysis sought to provide a more holistic view of the problem and the use of interviews and surveys served as an attempt to triangulate and attain a more comprehensive foundation of knowledge on which to base recommendations. With the methodology outlined in this chapter, the next chapter comprised analysis of each secondary question and analyzed subcomponents of the questions to arrive at answers to synthesize into an answer for the primary research question about DoD reform to support a whole-of-government approach to competition with Russia in the IE.

CHAPTER 4

ANALYSIS

Introduction

Using the methodology outlined in the previous chapter, the author distilled the nature of the Russian threat in IE in the gray zone and during open conflict. The Russo-Ukrainian War case study answered the first secondary research question of how Russia employed information to support military activities in Ukraine. The resulting answer framed the problem against which the author sought to address with recommendations in chapter 5.

The author sought to employ methodologies outlined in chapter 3 to generate new data to combine with the knowledge gained in the conduct of the literature review to analyze data and determine answers to two secondary research questions. Then, the author synthesized that new information and answered the primary research question to identify areas in which the DoD must reform to better conduct operations in the IE in support of the USG.

From the literature review, scholarly works demonstrated Russia's informational components of NGW and how Russia exploited digital and social media during gray zone activities to set advantageous conditions in Crimea and the Donbas prior to overt military operations in 2014. This activity aligned with the information/psychology side of Russian IW. Once kinetic military operations began, Russia brought additional information/technology capabilities and activities to bear against Ukrainian forces and the population.

Russo-Ukrainian Conflict 2013-2017

Since the dissolution of the Soviet Union in 1991, Russia and Ukraine engaged in competition that began as information warfare but in 2014 escalated to kinetic operations. First, Russia exacerbated political and social unrest by leveraging diplomatic, informational, and economic instruments of power in an undeclared conflict with Ukraine. Then Russia shaped the operational and information environments domestically by garnering the support and will of the Russian people; regionally, by demonstrating power and perception of legitimacy--at least to ethnic Russian audiences outside Russia; internationally, by doggedly pursuing a perception of legitimacy and demonstrating the capacity to be an influential power globally. Finally, Russia executed overt military operations beginning with the seizure and annexation of Crimea in 2014 followed by the invasion into eastern Ukraine by taking control of the Donetsk and Luhansk Oblasts. The information strategy supporting these operations included employment of multiple IRCs including psychological operations, deception, electronic warfare, cyberspace operations, public affairs, and intelligence.

To execute this information strategy, Russia used various themes designed for specific audiences to actively or passively support future Russian activities. The government centrally created their themes, and subordinate entities—military and non-military, in accordance with NGW—executed information warfare in a decentralized manner. Russian intelligence and special operations personnel executed this shaping in Ukraine through the use of digital and social media for propaganda purposes under the guise of social activism and change as well as by the development of proxy and surrogate networks. Initially, these activities were covert. However, Russian soldiers posted selfies

to social media and inadvertently helped expose Russian military involvement in Ukraine.[64] Russia's previous narrative of protecting the ethnic Russians on their frontier mitigated some damage from this exposure.

Consistent with the Russian way of war, the strategic approach to the information component of their NGW is aggressiveness and brute force that is bold, opportunistic and dynamic, and unconstrained by the truth. Another characteristic that gives Russia's information strategy strength is the decentralized execution of centralized themes without a cumbersome bureaucratic approval process.[65] As previously mentioned, this provided resilience when open source intelligence exposed their activities in Eastern Ukraine. To understand how Russia implemented its "new type warfare" in Ukraine, one must examine the ends, means, ways, and risks of the Russian strategy. The end is to compete with the West on the world stage and attrite the influence of Western states on its frontier countries; the means, which are the capabilities Russia employed in the IE; the ways, which is how Russia leveraged those capabilities; and the risks involved at the strategic to tactical levels.

To better understand how Russia implemented NGW in Ukraine, this paper uses the strategic, operational, and tactical levels of warfare as lenses. At the strategic level, Russia's capacity for mass delivery of content online and via traditional media outlets like television, radio, and print is significant. Putin has consolidated information efforts

---

[64] James M. Davitch, "Open Sources for the Information Age: Or How I Learned to Stop Worrying and Love Unclassified Data," *Joint Forces Quarterly*, no. 87 (4th Quarter 2017): 21.

[65] MAJ Jerome Petersen, interview by the author, Fort Leavenworth, KS, 27 April, 2018.

across multiple vectors to deliver disinformation to internal and external populations. For the near-external populations, mostly Russians in frontier countries, Russian media is the only information that caters to their language instead of the local media. If audiences only have access to one vector of information, they base their perceptions upon that narrative. They are also less likely to question the portrayed narrative or view alternate narratives.

Russia may employ violence to achieve information effects. For example, armed men seized the television and radio stations in areas of Ukraine, replacing Ukrainian channels with Rossiya 24, a Russian news channel.[66] This physical attack to affect information/technology (controlling the content delivery medium) was an interim step to affect information/psychology by controlling content delivered to target audiences within the cognitive dimension of the IE. This tactical action resulted in strategic effects by denying the audience access to other vectors of information like the Ukrainian channels through an information blockade.

At the operational level, use of surrogates and proxies to facilitate information warfare activity is another tool Russia employed. Local proxies provided credibility to the narrative, such as the Russian theme of "Novorossiya" or "New Russia" as a moniker for Eastern Ukraine. Also, Russia used paramilitary contractors in Ukraine to add a level of deniability to their activities. While many of these contractors could be prior service military or military-trained, their status as independent contractors allows more options within the geopolitical realm. For example, the recent deaths of Russian contractors in Syria who facilitated attacks on U.S. uniformed forces allowed both Russia and the U.S.

[66] Center for Strategic International Studies: Russia and Eurasia Program, "The Ukraine Crisis Timeline," accessed 21 February 2018, http://ukraine.csis.org/crimea.htm#6.

to refrain from overt military escalation due to the non-official capacity of the contractors.

At the tactical level, Russia employed technological capabilities in Ukraine for electronic warfare that can disrupt unit operations and enable friendly maneuver. These capabilities successfully disrupted communications and navigational systems. Another capability demonstrated by Russia at the tactical level is precision message delivery when setting tactical conditions in Crimea. Russia sent text messages directly to the cellular devices of some soldiers indicating threats to their families, affecting them psychologically and possibly contributing to the poor showing of the Ukraine security force's defense of Crimea. Russia again demonstrated this capability by taunting Ukrainian forces after an indirect fires barrage by sending text messages asking how they liked the artillery.[67]

[67] Center for Army Lessons Learned, CALL Handbook No. 17-09, *Russian New Generation Warfare* (Fort Leavenworth, KS: Center for Army Lessons Learned, 2017), 23.

Table 2. Comparison of terminology

USSR/Russia	USA/NATO
Reflexive Control	Perception Management
Maskirovka	Tactical Deception
Information Warfare	Information Operations
New Type War	NGW/Hybrid War (US-term); No parallel US term for equivalent activity
Radio Electronic Combat	Command, Control, Communications Countermeasures → Command and Control Warfare
Active Measures	Covert Action

Source: Created by author.

Ultimately, the threats identified in the case study are gray zone activities with surrogates and proxies, exploitation of social media, the EW and counterintelligence threat at the tactical level. These tactical threats include communication and navigation disruption, targeting of emissions with intelligence sensors that cue artillery barrages and airstrikes, PSYOP delivery via text message on personal devices, and foreign intelligence entity threats collecting on servicemembers via social media. This list is not all inclusive but serves as a basis against which to analyze DoD capability gaps within doctrine, organization, and leadership education to address these threats in the IE. Whether in the gray zone or large-scale combat operations, the DoD must be prepared to overmatch or counter these threats as part of its deterrence strategy and operations planning.

Analysis of DoD Information capabilities

The *DoD Strategy for Operations in the Information Environment*, published in 2016, outlined near; mid; and long-term outcome for the strategy. The near-term, between six and 18 months, focused on the "rapid, prioritized, high-impact changes to existing policy, doctrine, and professional military education and assessment efforts."[68] The only discernible change to information and joint doctrine during the near-term was the designation of information as a joint function in JP 1-0 in June 2017.[69] However, the current doctrine does not satisfactorily explain the implications of the new joint function according to survey data and interviewed personnel. The desired long-term outcome of the 2016 strategy is, "institutionalized and integrated operations in the IE. The [DoD] will field and manage a well-trained, educated, and ready IO and total-force to meet emerging requirements."[70]

In simple terms, IO is the synchronized, integrated employment of two or more IRCs in support of the Joint Force Commander's operations. COL Mark Vertuli stresses that that IO supports the commanders overall operational campaign plan to achieve ends through the integration of IRCs in planning and execution. He further states that it is not a separate planning effort, contrary to common perception.[71] Doctrine paints a picture that

---

[68] Department of Defense, *Strategy for Operations in the Information Environment*, 7.

[69] Joint Chiefs of Staff, Joint Publication (JP) 1-0, *Doctrine of the Armed Forces of the United States*, change 1 (Washington, DC: Government Printing Office, 2017), I-19.

[70] Ibid., 7.

[71] COL Mark A. Vertuli, interview by the author via telephone, 25 April, 2018.

IO is a capability on par with the other IRCs rather than a planning function to synchronize the discrete activities of the IRCs.

The USG must adopt a more effective whole of government or whole of nation approach to compete in the IE. The DoD must modernize and adapt to support synchronized unified action across the instruments of national power. Within the DoD, gaps exist in doctrine, organization, and education that present opportunities for reform to compete with Russia in the IE.

Doctrine

While change 1 to JP 1-0 introduces "Information" as a new joint function, it does not define it well with regard to its use. Unconventional Warfare, including sensitive activities and covert action, are covered in JP 3-05. Army IO doctrine is the most prevalently influential of the services and appears to provide the bulk of input to joint IO doctrine. Army doctrine spread information related capability tasks across multiple Warfighting Functions. Except for FM 3-13 *Information Operations*, multiple Army manuals confuse IO and IRCs, perpetuating confusion amongst servicemembers. For example, Army Doctrine Reference Publication (ADRP) 6-0 *Mission Command* lists staff tasks and additional tasks in the mission command warfighting function: synchronize information-related capabilities, conduct cyber electromagnetic activities, conduct military deception, and conduct civil affairs.[72] By listing a task to synchronize IRCs, which is essentially the definition of IO, and then listing tasks to conduct the discrete action of information-related capabilities rather than the synchronization of those

[72] Department of the Army, Army Doctrine Reference Publication (ADRP) 6-0, *Mission Command* (Washington, DC: Government Printing Office, 2014), 3-6.

activities detracts from the force's understanding of IO. This oversight also fosters a misconception that IO is "themes and messages" and that "cyber" is something unique and discrete from IO.

In this section, the author traces the evolution of definitions and doctrine through the emergence of IO in policy and doctrine from the mid-1990s to the current generation. Notable in figure 4 is the frequent and desynchronized modification to IO doctrinal manual related to capstone doctrine, and the number of changes to terminology for IO. The joint and service-specific doctrine for IO is consistent and clear but the capstone, operational and tactics doctrine, sows confusion on IO through incorrect diction.

Table 3. Survey Question 2 Response

Question 2: The addition of Information as a Joint Function in JP 3-0 is clearly defined in doctrine and through classroom instruction at CGSC.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
0	3	6	1	1

Source: Likert Scale display created author, bar graph generated by Ralph Reed's execution of the confidential online survey.

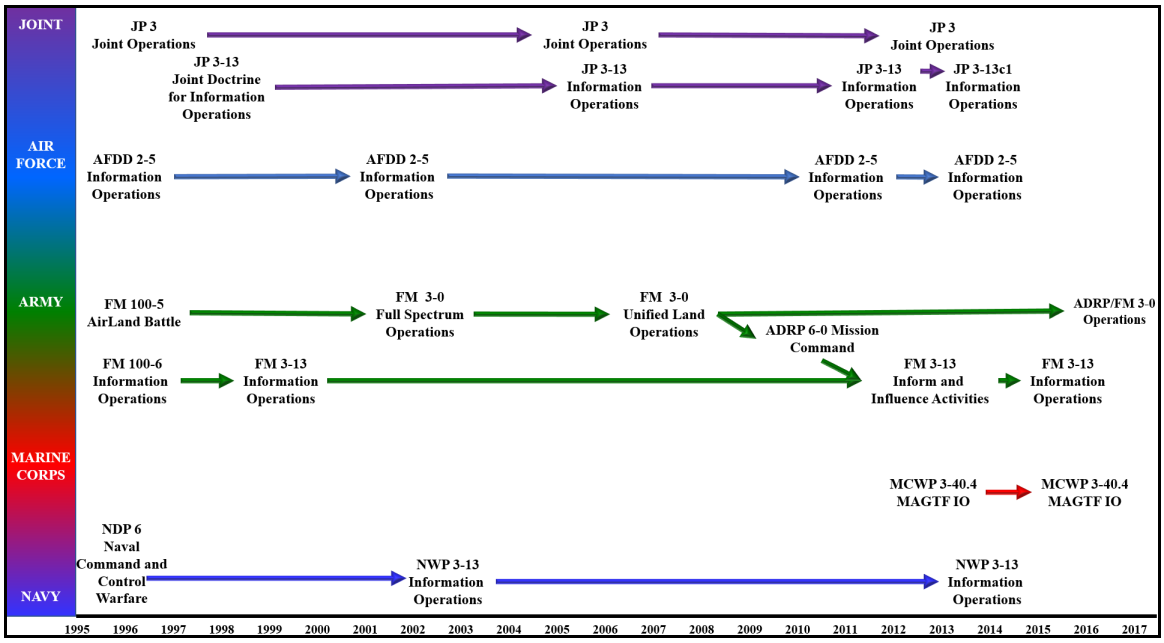


Figure 4. Historical Evolution of IO and Operational Doctrine

Source: Created by author.

Command and Control Warfare (1993)

As noted in Lowe's monograph, the concept of C2W, the original design function of what became IO, applied to large-scale combat operations and involved the employment of tools to disrupt or destroy the enemy's ability to command and control forces, while protecting friendly forces' ability to do the same. Targeting C2 nodes, communications infrastructure, and affecting adversary decision-making by increases the fog of war. The Soviet military centralized decisionmaking during this time.[73]

[73] COL Mark A. Vertuli, interview by the author via telephone, 25 April, 2018.

FM 100-6 Information Operations (1996)

Field Manual 100-6 was the first IO manual in the Army. It emerged as a complement to the capstone doctrine of the time- FM 100-5 *AirLand Battle*. The manual acknowledges the IE and proffers a definition for information dominance:

> The degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations short of war, while denying those capabilities to the adversary.[74]

2013 Version of FM 3-13 Inform and Influence Activities

This field manual highlights two lines of effort: the inform line of effort and the influence line of effort. The manual delineates the functions between inform and influence. As a result of the Global War on Terrorism and the heavy focus for the Army on counterinsurgency doctrine, much of the focus for IO in this version of FM 3-13 became population-centric, rather than adversary decisionmaker-centric in purpose. Soldier-Leader Engagement/Key Leader Engagement emerged as an IRC, and commanders of tactical units relegated the FA30s to that role.[75]

This manual also defined the purposeful roles of both inform:

> Commanders have responsibility to conduct public affairs operations that inform U.S. audiences about their military operations to the fullest extent possible. Using information-related capabilities such as public affairs, MISO, civil affairs operations, and others enables the commander to also inform foreign audiences and to provide Army support to strategic communication. Commanders balance

---

[74] Department of the Army, Field Manual (FM) 100-6, *Information Operations* (Washington, DC: Government Printing Office, August 1996), 1-9.

[75] MAJ Jerome Petersen, interview by the author, Fort Leavenworth, KS, 27 April, 2018.

> informing audiences about Army operations with the responsibility to protect those operations and their troops through OPSEC.[76]

and influence:

> IIA enable commanders in integrating and synchronizing the various means of influence to support operations. U.S. forces strictly limit their influence activities to foreign audiences. Influence activities typically focus on persuading selected foreign audiences to support U.S. objectives or to persuade those audiences to stop supporting the adversary or enemy. To accomplish operational objectives effectively, commanders may direct efforts to shape, sway, or alter foreign audience behaviors.[77]

This thinking is erroneous when viewed through the lens of the historical origins of IO. Neither of these lines of effort addresses the disruption of adversary command and control but rather focuses on the cognitive dimension of the adversary or the foreign population. This likely resulted from the operating environment of the Global War on Terrorism that had been ongoing for 12 years at that time. The focus of FM 3-13 was too much towards the "Battle of Ideas" presented by Lowe and does not incorporate the original functionality of where "IO" came from, which was to support "Battle." This omission may have been a deliberate decision in an attempt to split IO into Inform and Influence Activities and Cyber Electromagnetic Activities.

In figure 5, the author modified the phasing model for joint operations to show when the IO main effort between the ideas of C2W and the "battle of ideas" lay in relation operational phases. The solid boxes represent gray zone and low-intensity phases wherein information activities executing the "battle of ideas" is critical. The dashed box around phases two and three represent when C2W activities are most vital.

---

[76] Department of the Army, Field Manual (FM) 3-13, *Inform and Influence Activities* (Washington, DC: Government Printing Office, 2013), 1-2.

[77] Ibid.

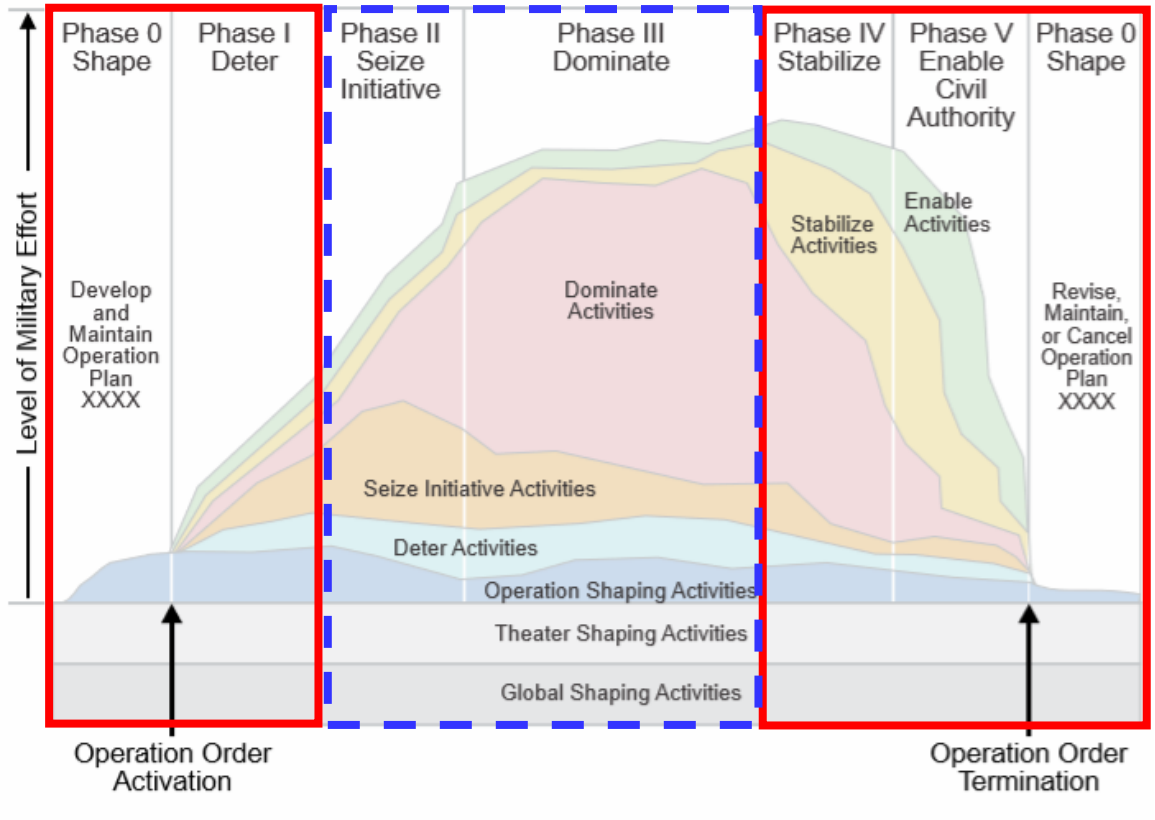


Figure 5. U.S. Military Joint Operations Phasing

Source: Joint Chiefs of Staff, Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: Government Printing Office, 2017), V-13.

2008 Version of FM 3-0, *Unified Land Operations*

The 2008 version of the Army's capstone doctrine, FM 3-0 *Unified Land Operations*, was significant to IO. It brought information and civil support tasks to the force on par with the offense and defense.[78] The 2008 FM 3-0 stated, "the impact of the

[78] Thomas Rid and Marc Hecker, *War 2.0*: *Irregular Warfare in the Information Age* (Westport, CT, Praeger Security International, 2009), 3.

information environment on operations continues to increase."[79] Also, the term "information superiority" emerged with a full chapter dedicated to it.

However, the term information superiority may be misleading. Given perception that having the upper hand in the battle of the narrative or ideas equates to achieving information superiority. An accurate meaning attributable to this term relates back to C2W and the ability to negatively impact the adversary's ability to command and control its forces while protecting friendly ability to conduct mission command.

2017 Version of FM 3-0, *Operations*

This manual directs significantly more attention to the IE and IO than previous incarnations. The manual does not confuse IO with IRCs. Figure 6 depicts the employment of IRCs with a lens toward large-scale combat operations using time and phasing as the main axis. However, it fails to account for physical space in the operational environment. There are many aspects of IO that will occur in the consolidation area simultaneously with large-scale combat close to the front lines. Doctrine in general as in figure 6 does not articulate what comprises "messaging." There is ambiguity as to whether it refers to Military Information Support Operations (MISO) messages, Public Affairs products, Soldier Leader Engagement or Key Leader Engagement talking points and who must be responsible for the synchronization of them. Given that figure 6 lists MISO as a separate capability from messaging, there is less clarity.

[79] Department of the Army, Field Manual (FM) 3-0, *Operations* (Washington, DC: Government Printing Office, 2008), viii.

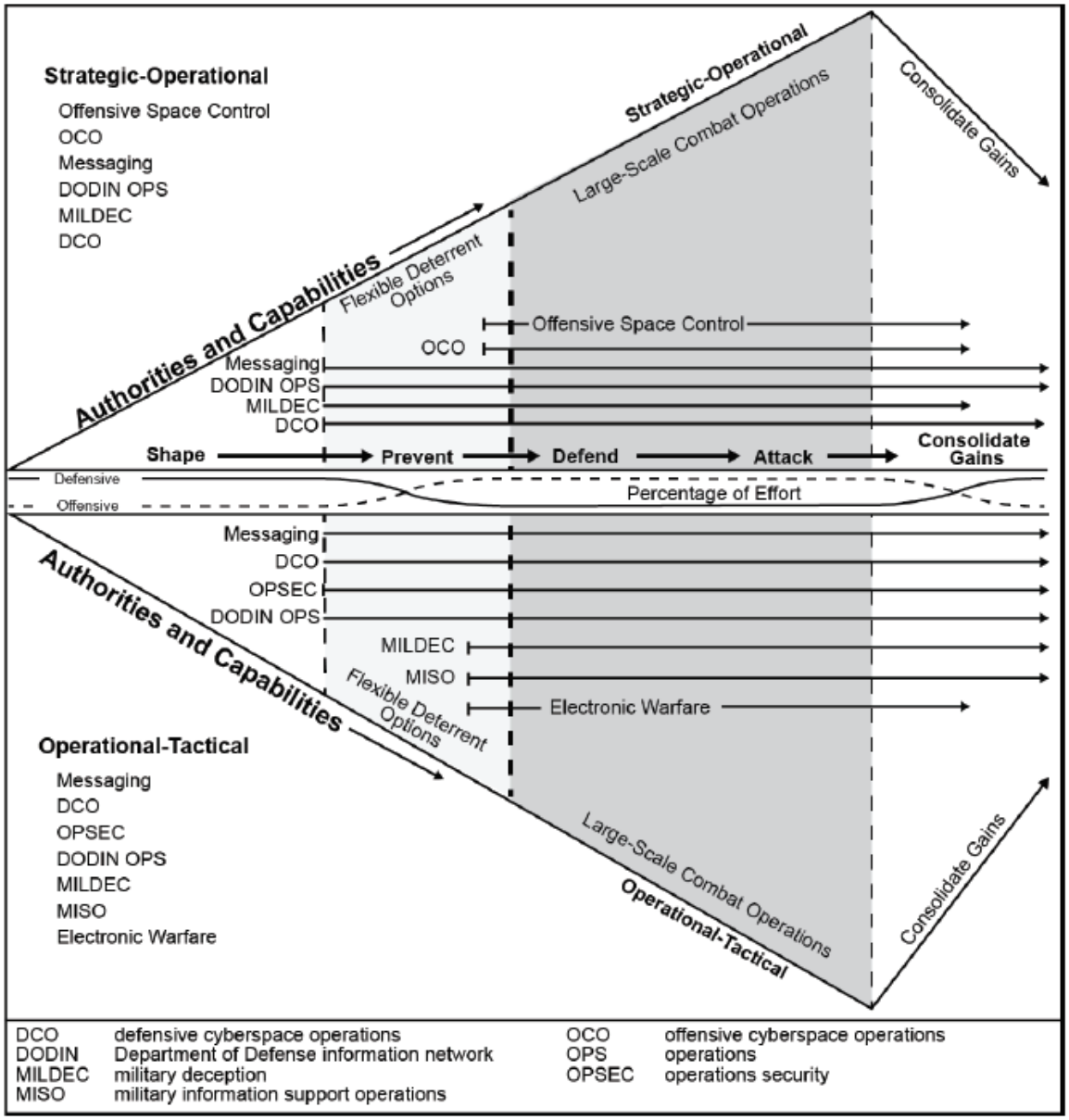


Figure 6. Dynamic Continuum of Information Operations

Source: Department of the Army, Field Manual (FM) 3-0, *Operations*, Change 1 (Washington, DC: Government Printing Office, 2017), 2-27.

Other examples of joint policy and doctrine that present opportunities for confusion on IO include Chairman of the Joint Chiefs of Staff Instruction (CJCSI)

3210.01C Joint Information Operations Proponent and Joint Doctrine Note 2-13 *Commanders Communication Synchronization*. Figure 7 depicts a visualization from the 2013 Joint Doctrine Note for which shows IO as a capability with the other listed IRCs, rather than the integration of IRCs as defined in DODD 3600.01 and JP 3-13 *Information Operations*.

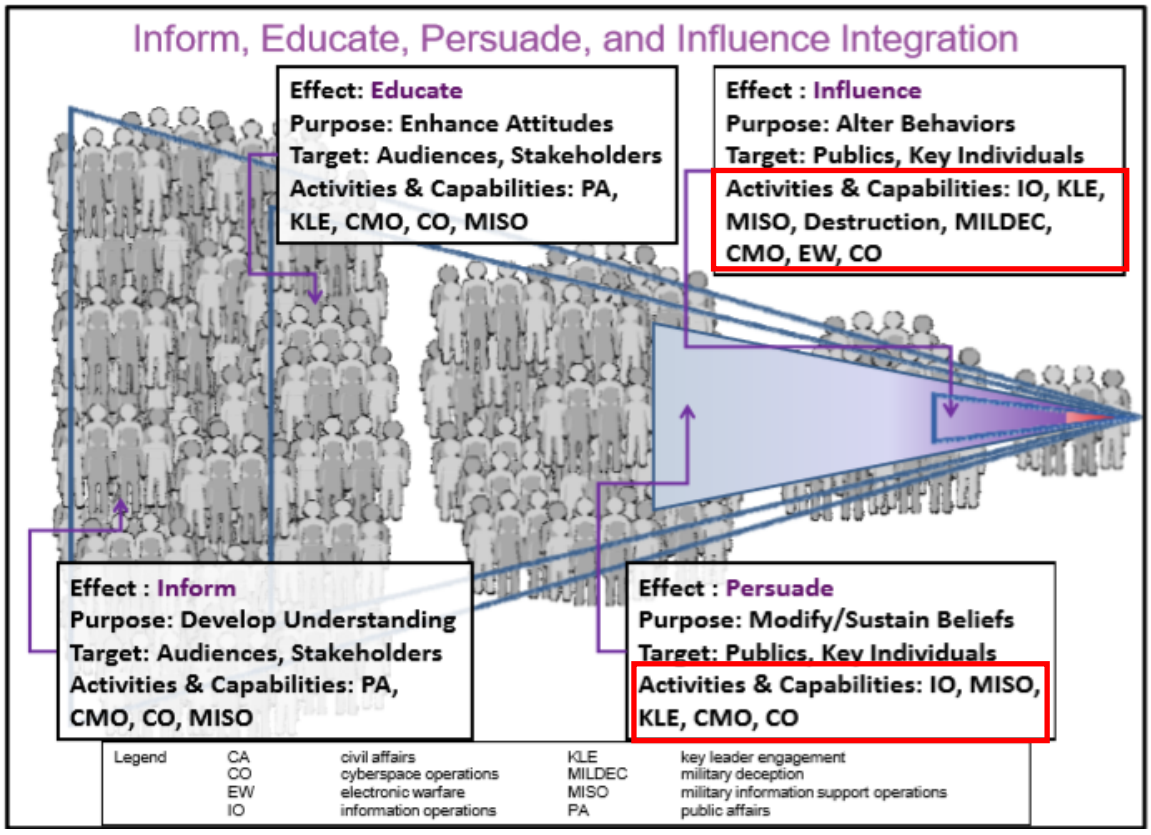


Figure 7. Desired Effects of Commander's Communication Synchronization

Source: Joint Chiefs of Staff, Joint Doctrine Note 2-13, *Commander's Communication Synchronization* (Washington, DC: Government Printing Office, 2013), I-13. Modified by the author.

Another instance in policy mislabeling IO as an IRC is CJCSI 3210.01C:

> j. Evaluate IRCs (including IO, SC, CO, MISO, PA, and VI) needed to lead organizational change and transformation in order to build and sustain innovative, agile, and ethical organizations in a joint, interagency, intergovernmental, and multinational environment.
> k. Analyze the integration of IRCs in support of IO, SC, MISO, and PA objectives during their employment as a part of theater campaign execution, including pre- and post-conflict operations.[80]

Given the joint doctrinal definition of IO, these examples contradict that IO is the integration of IRCs—including Public Affairs—during military operations, even in phase zero.

In addition to the conflicting terminology with regard to IO and IRCs, a current disconnect exists between joint doctrine, which has Information as a Joint Function, and Army doctrine, which has information as an element of combat power. Therefore, Army doctrine does not yet align with joint doctrine. Implications for information not becoming a Warfighting Function is that there are not dedicated resources like a Center of Excellence to act as the proponent of the function, set the education of its professionals, and to codify its specific doctrine.

General David Perkins, former U.S. Army Training and Doctrine Command commander, devised the initial concept of multi-domain battle as the next evolution of AirLand Battle and Unified Land Operations. The evolution of doctrine to support the multi-domain battle concept, if validated, should inherently force the Army to adopt a more "joint" approach to operations given that successful operations across the different operational domains rely on inter-service coordination. However, another change in

[80] Chairman of the Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01C, *Joint Information Operations Proponent* (Washington, DC: Government Printing Office, 2014), E-2.

doctrine could contribute to more confusion across the force if not done in conjunction with joint and service capstone doctrine.

Organization

One glaring gap is the lack of command synchronization across information activities within the DoD. United States Cyber Command (USCYBERCOM) exists to manage the DoD cyberspace activities conducted under the authorities of Title 10 of the United States Code. Title 10 grants authorities to the Armed Forces to conduct their operations and activities.

Another gap in organizational structure is the myriad of service perspectives on where IO should align, who controls the component IO commands, and command relationships and involvement of higher echelons. Figure 8 depicts most of the DoD IO enterprise as the author understands. The figure offers a glimpse as to the enormity of the IO bureaucracy and begins to provide context to why change will be cumbersome. Each service has its specific interests and generally are unlikely to cede control of resources if possible.

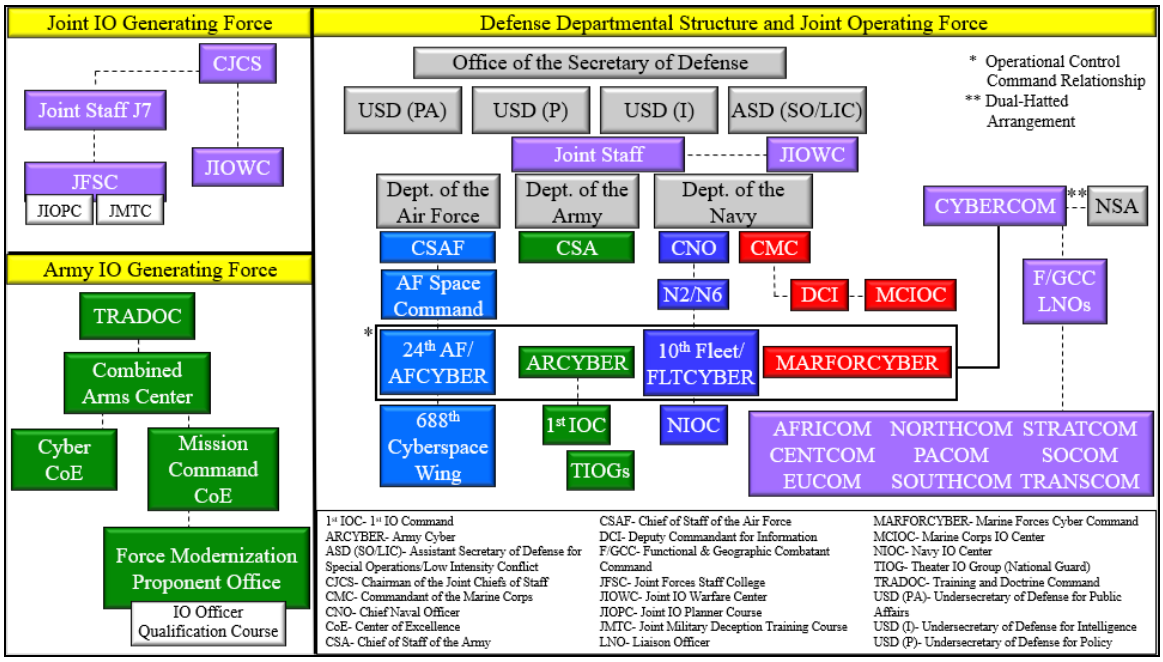


Figure 8. Current DoD IO Enterprise

Source: Created by author.

The U.S. Army is the only service with IO Professionals in the form of the Functional Area 30 (FA30) officers in addition to Information Capability Specialists, who are the career specialists of the various IRCs. The other services within the joint force have Information Capability Specialists but no career field that integrates and synchronizes the efforts of the IRCs in support of the commander's plan. However, servicemembers can serve as trained IO planners in joint organizations once they graduate from the Joint Information Operations Planner Course hosted by the Joint Forces Staff College located in Norfolk, Virginia.

With regard to Service policy and organization, the Army places the function of the IO professional under the Operations, or S/G3 staff directorate. In the past, it stood alone as the S/G7 directorate. The lowest echelon at which an IO professional serves is

the division-level in conventional Army units. With the loss of IO professionals at the brigade level, commanders and staffs do not realize how they could leverage information related capabilities to enable large-scale combat operations, or recognize and respond to threats at the tactical level.

Navy policy on IW resides in the N2 and N6, intelligence and communications staff directorates, respectively, under the umbrella of "information dominance." Navy IO focuses predominantly on EW and Cyberspace IRCs. In the context of Lowe's monograph, it makes sense that the Navy's approach to IO is more focused on the original functional design of IO from the Cold War that targeted ability to disrupt adversary command and control. The other land component force that interacts with the human terrain in operations is the Marine Corps. While the Marine Corps does not have a dedicated career field for IO, the Marine staffs place their planner with responsibility for IO in the future operations cell of the S/G3.[81] The Marines resemble the Army most in proficiency and capacity to account for the plethora of IRCs in planning at the tactical and operational level.

Of the five "IO commands" in the defense enterprise, three of them are under the operational control of the service component cyber command. The Army's 1st IOC, located at Fort Belvoir, Virginia, is subordinate to Army Cyber (ARCYBER) and the Intelligence and Security Command. The Marine Corps Information Operations Command is directly subordinate to the newly created position within the Marine Corps of Deputy Commandant for Information.

---

[81] U.S. Marine Corps, MCWP 3-40.4, *Marine Air-Ground Task Force Information Operations* (Washington, DC: Government Printing Office, 2013), 2-1.

The Naval Information Operations Center, located in Norfolk, Virginia is under Fleet Cyber Command. The Air Force's 688th Cyber Wing, located in San Antonio, Texas is subordinate to 24th Air Force, the Air Force cyber component.

The 688th's mission is to "operate, integrate and win in the cyberspace, electromagnetic spectrum and space domains."[82] This unit previously had the designation "688th Information Operations Wing." The re-designation of the wing as a "Cyber Wing" reinforces that assertion that the Air Force focuses predominantly on the technological aspects of IO like the EW, Cyberspace Operations, and Special Technical Operations IRCs.

The Joint Information Operations Warfare Center (JIOWC) is subordinate directly to the Joint Staff as a Chairman's Controlled Activity. In years past, the JIOWC provided trained and ready IO planning capacity to joint operational forces, but recently the JIOWC refocused its efforts to directly supporting the Joint Staff.[83]

Because information is not an Army Warfighting Function, the IO proponency for Force Modernization is subordinate to the Mission Command Center of Excellence. As a result, the colonel that is responsible for the IO proponent has five "hats" as the proponency for Knowledge Management, IO, Military Deception (MILDEC), Operations Security (OPSEC), and Personnel Recovery as well. These additional obligations detract from the limited time and resources that could focus on improvement of the Army's ability to operate in the IE.

---

[82] U.S. Fleet Cyber Command, "Homepage," accessed 29 April, 2018, www.public.navy.mil/fcc-c10f/Pages/home.aspx.

[83] MAJ Jerome Petersen, interview by the author, Fort Leavenworth, KS, 27 April, 2018.

There are two functional combatant commands that have significant potential relevance to information operations and the information environment: USCYBERCOM and United States Special Operations Command. The USCYBERCOM has responsibility for conducting operations in the cyberspace operational domain and is wholly focused on the IE. The United States Special Operations Command has 11 doctrinal core activities of which nearly all impact the IE including IO, MISO, Unconventional Warfare, and Civil Affairs Operations, Foreign Internal Defense, Foreign Humanitarian Assistance and Security Force Assistance. These activities could create opportunities for strategic and operational advantages during pre-conflict periods, or the "gray zone."

Leadership Education

The CJCSI 3210.01C states, "PME institutions are responsible for IO-focused education for members of the general military population and the [Joint IO Force]."[84] In general, servicemembers do not understand the complexity of the information environment, nor are the PME institutions adequately ameliorating the problem. Information operations planners often hear, "just go do some IO," or "what is IO doing about this?" Many do not even understand that the FA30/IO Officer is merely a staff officer charged with the coordination and integration of the activities of the IRCs in a synchronized manner to best support the commander's operations. An IO Officer does not have authority to direct execution of activities, nor does he or she own the capability that does execute.

[84] Chairman of the Joint Chiefs of Staff, CJCSI 3210.01C, *Joint Information Operations Proponent*, A-8.

With regard to leadership education, policy and doctrine should dictate educational requirements and which organizations had educational responsibility. Currently, only the National Defense University and the Naval Postgraduate School have Joint IO Proponent-approved IO programs.[85] The IO Career Force according to Department of Defense Instructions and 2006 version of JP 3-13 should "consist of both capability specialists (EW, PSYOP, [Cyber Network Operations], MILDEC, and OPSEC) and IO planners: [86]

> The development of IO as a core military competency and critical component to joint operations requires specific expertise and capabilities at all levels of DOD… At each level of command, a solid foundation of education and training is essential to the development of a core competency. Professional education and training, in turn, are dependent on the accumulation, documentation, and validation of experience gained in operations, exercises, and experimentation.

While there is a plethora of course within the DoD for Information Capability Specialists, there are only three for IO Planners: Joint Information Operations Planner Course, the Tactical IO Planner Course, and the FA30 Qualification Course. With regard to professional military education, the 2018 National Defense Strategy states:

> PME has stagnated, focused more on the accomplishment of mandatory credit at the expense of lethality and ingenuity. We will emphasize intellectual leadership and military professionalism in the art and science of warfighting, deepening our knowledge of history while embracing new technology and techniques to counter competitors. PME will emphasize independence of action in warfighting concepts to lessen the impact of degraded/lost communications in combat. PME is to be

---

[85] Chairman of the Joint Chiefs of Staff, CJCSI 3210.01C, *Joint Information Operations Proponent*, D-4.

[86] Joint Chiefs of Staff, Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: Government Printing Office, 2006), xv.

used as a strategic asset to build trust and interoperability across the Joint Forces and with allied and partner forces.[87]

Table 4. Joint IO Operations Force Requirements

Level of War	Functional Level	Billet Title	Rank					Jt IO Ed & Tng	
			E-6/7/8 E-9	O-4 O-5	O-6	O-7 8/9	CIV	JIOPC	SJIOAC
Strategic	JOINT STAFF J-38	IO Coordinator		X			X	X	
		Branch Chief		X				X	
		Division Chiefs			X			X	
		Deputy Director*				X			X
Strategic/ Operational	CCMD HQ Staff	IO Coordinator	X	X			X	X	
		IO Division/Branch Chief		X	X		X	X	
		Deputy Director for Operations*				X			X
	CCMD SOC	IO Coordinator	X	X				X	
		IO Division or IO Branch Chief		X	X			X	
Operational/ Tactical	JTF/JFC	IO Coordinator	X	X	X			X	
		Commander*				X			X

Source: Chairman of the Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01C, *Joint Information Operations Proponent* (Washington, DC: Government Printing Office, 2014), F-1.

In table 4, the CJCSI outlines the rank and education requirements for Joint IO billets at the various echelons of headquarters. Figure 8 highlights the three main Joint and Army qualification courses that certify IO practitioners to serve as IO and deception planners: Joint IO Planner Course, Joint Military Deception Training Course, and the Army's FA30 (IO) Qualification Course. These courses represent required gates to meet

[87] Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, 8.

when serving in IO Planner positions, per table 4 and various combatant commander's policy.

Leadership education within the DoD specifically professional military education is woefully deficient in developing an understanding of IO across the force.[88] There is only one contact hour of formal Information Operations instruction at the CGSC, at Fort Leavenworth, and that instruction does not typically come from an IO officer due to the limited number of them on staff- there are currently three. Instead, Special Forces, Civil Affairs, and Psychological Operations officers instruct the lesson due to availability and close working relationship of those branches with IO, institutionally. Compared to the 12 weeks, or 480 hours of instruction and practical exercises at the Information Operations Qualification Course for IO officers current IO instruction in Officer PME is deficient. This disparity means that at the brigade and battalion level, where the bulk of officers serve after graduation from CGSC, personnel have little to no education on IO that is not self-directed. Even at the division level, there may only be a few officers who have completed the 12-week course and that division assignment is their first as IO professionals. This may present a significant risk for error when operating in the IE as actions at the tactical level can have strategic impacts, such as the Russian soldiers posting to social media in Ukraine, or U.S. soldiers burning a Qur'an in Afghanistan.

At the Joint Forces Staff College in Norfolk, Virginia, the personnel selected to attend the Joint Information Operations Planner Course spend four weeks delving into joint information operations with a curriculum based on joint doctrine and with additional

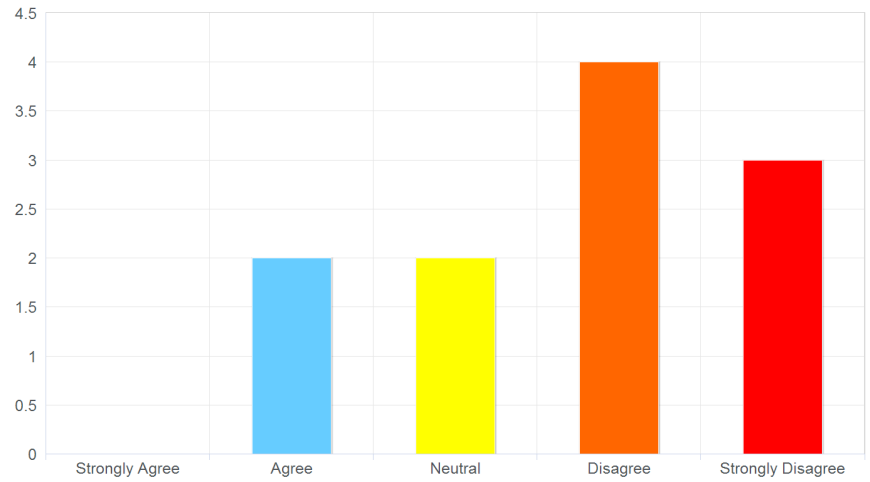
[88] LTC Amy Burrows, interview by the author, Fort Leavenworth, KS, 24 April, 2018.

emphasis placed upon Joint IO, Joint OPSEC, and Joint MILDEC. However, attendance is primarily for personnel currently assigned to Joint IO billets or identified for that role in a future assignment.

Table 5. Survey Question 4 Results

Question 4: I had a good understanding of Information Operations prior to attending Command & General Staff College.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
0	2	2	4	3



Source: Likert Scale display created author, bar graph generated by Ralph Reed's execution of the confidential online survey.

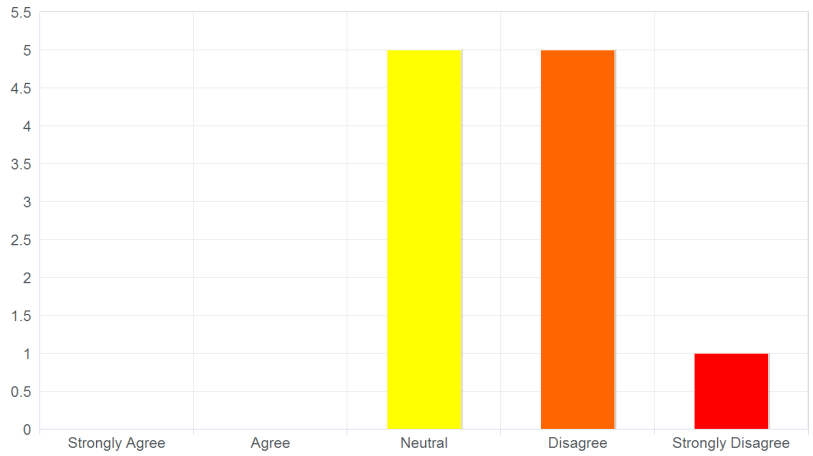
Tables 5 and 6 depict negative trends of understanding IO and the quality of emphasis placed on it in PME. Reinforcing this is the fact that less than 50 percent of the survey participants correctly answered that the IO Officer serves in the Operations staff

directorate of a headquarters.[89] When asked to define IO in their own words, only two of the respondents captured the essence of the doctrinal definition, while others plainly said they were "not sure" or called them intelligence operations.[90]

Table 6. Survey Question 1 Results

Question 1: The formal instruction on Information Operations I received at Professional Military Education has been sufficient.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
0	0	5	5	1



Source: Likert Scale display created author, bar graph generated by Ralph Reed's execution of the confidential online survey.

[89] Results of Survey Question 3.

[90] Results of Survey Question 6.

The results of the survey support the assertion that PME-at least Army CGSC-does not adequately provides officers with the knowledge and understanding required to successfully plan and integrate operations in the IE as part of the commander's operational plan. While the results are not conclusive evidence given the small sample size, the data does provide indicators that interviewees reinforced during this research.

Summary

Russia is politically unconstrained and governmentally synchronized in their approach leveraging social media, surrogates and proxies, deception, and EW as elements of NGW in Ukraine. The Russian military has integrated IO effects with their kinetic operations evidenced by the use of intelligence sensors like Unmanned Aerial Systems and signals detection to cue and mass kinetic and non-kinetic actions like artillery and psychological messages. In this example, Ukrainian soldiers noticed an unmanned drone overhead followed shortly by a devastating artillery barrage and subsequent taunting messages delivered to their personal electronic devices the Russian ability to dynamically and effectively integrate IRC employment with fires at the tactical level.

During the 1970s, the U.S. military adapted to Soviet Radio Electronic Combat doctrine and developed command, control, communications countermeasures which evolved into C2W and then IO. The military could enact these changes because senior leaders empowered commanders and organizations to assess their environments, assume prudent risk, and take action within the high commander's intent. The Soviets were bogged down by bureaucracy and micromanaged decision-making to adapt in the later stages of the Cold War environment, allowing the United States to gain advantageous capabilities in the IE. Over the course of the 1990s and the Global War on Terrorism, the

pendulum swung the other direction toward the Russians who are much more capable of operating in the IE than previously and are less constrained by bureaucracy. The Russians employ the instruments of national power in a more effective and synchronized manner in a whole-of-nation approach.

Through analysis of the two secondary research questions, the author concludes that the DoD should execute reforms within doctrine, organization, and leadership education, among other elements of DOTMLPF-P to improve its contribution to unified action against Russia in the IE. Within the DoD, the joint and service doctrine diction lends to the misperception about IO that exists in the force. In many of the essential tactics and operations manuals, IO appears to be an IRC on par with the others rather than as an integrating staff function. This misunderstanding stems in part from the divergence of the original functional design of IO as a way to conduct C2W, as highlighted by Lowe. Despite a generally consistent definition of IO in IO doctrine and policy, lack of education and integration also contributes to the muddling of what IO is over the past 25 years. The heavy focus on counterinsurgency operations also was a significant factor without adequate education in PME on IO led to lack of understanding of IO.

In the near term, the DoD needs to counter the EW threat by relearning previously common proficiencies such as tactical deception and emissions control. The DoD must decide what will be encompassed in IO regarding functionality and unify IO DoD-level efforts under a combatant command while the theater-strategic and operational level activities are the responsibility of the Geographic Combatant Commands (GCCs). Finally, a capability gap for education is evident. The military education enterprise does not appear to have adequate resources to adhere to the Secretary of Defense's guidance to

promote better education and awareness of conflict and future threats in the Information Age. By addressing the identified capability gaps in doctrine, organization, and leadership education, the DoD can improve servicemembers' understanding of IO within the IE. Using the Army Leader Development Model, the author proposes to frame reforms regarding the three domains depicted in Figure 9: operational, institutional, and self-development. Reforms in doctrine can improve leader self-development, changes to organizational structures can facilitate improved effectiveness in operating in the IE through the operational domain, and changes to PME can improve institutional leader development. Additionally, doctrine and PME reforms will have direct effects and ultimately, indirect positive effects in the operational domain over time as generational cohorts of officers promulgate the force after improved institutional and self-development efforts.

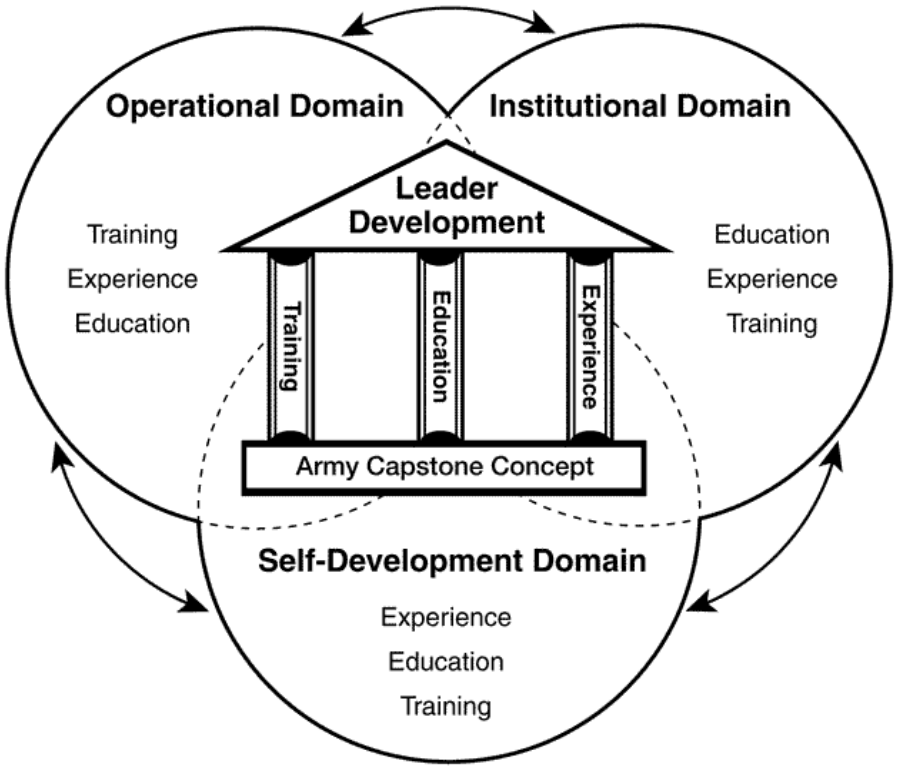


Figure 9. Army Leader Development Model

Source: David Hodne, "Accruing Tacit Knowledge: A Case for Self-Study on behalf of Professional #Leadership," The Strategy Bridge, 3 April 2016, accessed 26 April 2018, https://thestrategybridge.org/the-bridge/2016/4/3/accruing-tacit-knowledge-a-case-for-self-study-on-behalf-of-professional-leadership.

Then-COL Hodne explained the three domains of the Army Leader Development Model depicted in figure 9:

> The operational domain includes experience gained during contingency operations, training activities at home station, rotations at a Combat Training Center, or unit level leader professional development sessions. The institutional domain accounts for attendance at schools and professional military education (PME) to obtain knowledge, skills, and practice necessary to perform critical tasks. Both the operational domain and the institutional domain develop leaders in establishing explicit knowledge, easily codified and articulated. The self-development domain is an individual responsibility and consists of independent

> study to enhance learning in the operational and institutional domain, address gaps in skills and knowledge, or prepare for future responsibilities.[91]

With clarified doctrine and greater inculcation of IO into PME curricula throughout officer and non-commissioned officer career paths, the joint force can begin to develop a better understanding of IO and its integration into operational plans. These two changes would directly impact the institutional and self-development domains and indirectly affect change in the operational domain of leader development. A more educated and aware force can execute operations in the IE in support of the commander's objectives better during training and operations. Ultimately, improved understanding of the IE could positively affect what Scharre noted about resistance to cultural understanding of the paradigm of war in the Information Age. A DoD more aware of IE considerations for operations and strategy can better support unified action at the national level.

[91] David Hodne, "Accruing Tacit Knowledge: A Case for Self-Study on behalf of Professional #Leadership," The Strategy Bridge, 3 April 2016, accessed 26 April 2018, https://thestrategybridge.org/the-bridge/2016/4/3/accruing-tacit-knowledge-a-case-for-self-study-on-behalf-of-professional-leadership.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

> The paradox of war is that an enemy will attack any perceived weakness. So we in America cannot adopt a single preclusive form of warfare. Rather we must be able to fight across the spectrum of conflict.
>
> — Secretary of Defense James Mattis, attributed to Colin Gray

Conclusions

Throughout this thesis, the author analyzed what the DoD must do to improve the ability of the defense enterprise to compete with Russia in the IE based on a case study of Russian NGW in Ukraine. The analysis focused on the need for the DoD to reform doctrine, organization, and leadership education to improve understanding of IO within the IE.

In conclusion, Russia found initial success in its strategy in Ukraine but this success hinged on two factors: deniability of its involvement and the unpreparedness of Ukrainian forces to operate on par with Russian forces in the operational and information environment. As intelligence experts exposed Russian involvement to the international community, Russia lost some freedom of action in the IE and lost legitimacy to international audiences. However, to domestic and some regional audiences' acceptance of the Russian identity narrative, the strategy gained legitimacy as ethnic Russians actively or passively supported Russia actions. Additionally, once Ukrainian forces adapted to Russian tactics of employing electronic warfare and other information capabilities in conjunction with kinetic activity, Russia lost the initiative and the Russo-Ukrainian war devolved into a "frozen conflict."

A question arises from this analysis: Can Russia replicate this success? The answer will likely depend on geography, ideological similarities, and military capability. Russia may only find success with NGW in frontier states because of the ethnic, religious, and language ties. The most likely venue in which NGW could occur in the future is the Baltic states. South American and Middle Eastern audiences will likely not be receptive to the Russian identity narrative, so Russia will have to modify its information strategy to achieve credibility of the message, or it must leverage other instruments of national power more heavily. Also, Western states represent more advanced military capabilities to operate in the IE and kinetically, where Ukraine did not, nor was Ukraine entitled to the legal benefits of the NATO alliance. This no doubt factored into Russia's risk calculus. Further, Russia demonstrated capabilities and intent during the Russo-Ukrainian War and the West learned lessons from observation, meaning Russia's adversaries took note and will be more prepared than Ukraine, should another conflict arise.

The analysis supports the conclusion that the DoD does not adequately understand and define IO within the IE. The defense enterprise has a mantra that "words have meaning" and the services do not use consistent terminology to talk about operations in the IE. Some of the most common misunderstandings are that IO consists of "themes and messages" or that IO is dropping leaflets. Only two IRCs develop "themes and messages:" Public Affairs (PA) and MISO. Another misperception is that IO is a separate

planning effort- it is not. If a plan goes to a commander for approval without the IO concept of support, then it is an incomplete plan.[92]

With regard to joint and service doctrine, a disconnect remains despite scholars' previous recommendations. While all the services have IO doctrine, the core information tasks for certain services tend toward the technical aspects of operations in the IE such as Cyber, EW, and Special Technical Operations. The Navy and Air Force fit the bill for this assertion. However, it is not wholly inappropriate for these Services to focus on component-level planning because they do not consider human terrain as much as land component forces must during joint operations. Rather, personnel of those services would rely on joint doctrine if serving on a Joint Task Force staff in an IO planner or operations officer capacity. Army and Marine Corps IO officers must consider not only the technical capabilities that affect the IE but the human cognitive dimension of the IE. The Army and Marine Corps IO doctrine reflect this as both services' doctrines more robustly consider cognitive effects in the IE. Whether during large-scale combat operations, limited contingency operations, security cooperation activities, or gray zone activities, the land forces must account for the technical and psychological aspects of IO.

Recommendations

The first step moving forward toward a long-term strategic solution is that the DoD must conduct a full-scale Capabilities-Based Assessment through the Joint Capabilities Integration Development System process to fully comprehend the capability gaps that exist in a holistic, comprehensive manner, rather than the piecemeal adoption of

[92] COL Mark D. Vertuli, interview by the author via telephone, Leavenworth, KS, 25 April, 2018.

initiatives like the creation of USCYBERCOM. Only with the joint force coming together to analyze and determine the gaps and seams between the services can the different branches of service achieve unity of effort in reforming the DoD to better support a whole of government approach to operating in the IE.

Secondly, the DoD should adopt the branding of "Operations in the Information Environment" instead of the term IO, which has negative or misunderstood connotations from warfighter experience during the current global war on terror and military operations other than war in the 1990s. While the American way of war is firepower and technology focused, the DoD must continue to expand the force's understanding of, and ability to operate in, the IE.

The DoD must make several changes to prepare for the threats Russia presents in the IE. First, the DoD must unify the Armed Forces services' understanding of what IO is and their responsibilities in the IE. "Information" is such a broad term and the DoD must define its contributions to a whole of government approach, coordinated with the interagency across the instruments of national power. Additionally, the DoD must improve dialogue and interoperability with the interagency enterprise, specifically those with such a vested interest in the IE like the Department of State, with their GEC's counter-propaganda role, the Central Intelligence Agency, the Broadcasting Board of Governors, and the Department of Treasury.

Doctrine

Within the Army, the creation of an information warfighting function would help codify IO tasks and provide it with a greater degree of importance with the Service. Also, it would allow the U.S. Army Information Proponent Office to better and more regularly

interact with 1st IO Command at Fort Belvoir to improve the training and operational planning support to the Army.

Within the Army capstone doctrine, FM 3-0 *Operations*, and the other tactics doctrine such as FM 3-90-1, *Offense and Defense*, and FM 3-90-2, *Reconnaissance and Security Tasks*, and FM 3-07, *Stability*, the doctrinal proponents should incorporate more language into the sections on planning considerations and assessments rather than simply acknowledging that there is an IO manual and referring readers to it. By having this additional language in the foundational manuals, the likelihood that non-IO professionals will give more consideration to enabling operations in the IE and motivation for additional self-directed study on the topic may increase. For the Navy and Air Force, the author proffers that no changes are necessary to their service IO doctrine in the near-term.

Organization

The author proffers three recommendations for organizational reform exist as a result of this research. The DoD should request legislation to change USCYBERCOM to United States Information Command (USINFOCOM) at Fort Meade, Maryland, as organizational change may force cultural change in thinking; reestablish tactical deception units, which can support theater efforts against near-peer adversaries in declared conflict; and modify brigade tables of organization and equipment to include a Functional Area 30- IO officer, or recode some maneuver and intelligence officer billets to include IO qualification requirements for that billet.

First, while this idea may sound heretical and onerous, reorganization of USCYBERCOM to be responsible for DoD Information Operations might provide the impetus to unify service efforts in the IE to best support a whole-of-government approach

to competing with adversaries. The Defense Information School, which trains organizational communicators like public affairs and combat camera personnel, and USCYBERCOM infrastructure is already at Fort Meade. The command would have a coordinating relationship with JIOWC as the training and force provider for Joint Force Commanders requiring additional IO planning capacity, and these expeditionary personnel would already have a working relationship with their parent unit at USINFOCOM.

The commander of USINFOCOM would remain a four-star general or flag officer, and the commander of the joint cyber entity would be a three-star general or flag officer. This three-star commander would also serve as the Deputy Commanding General for Cyber for the unified combatant command. Given the technical nature of cyberspace and electronic warfare tasks, the Deputy Commanding General-Cyber would have responsibility for what was once C2W, and therefore activities and cyberspace and the electromagnetic spectrum at strategic levels. The other Deputy Commanding General for Influence would have responsibility for IRCs aimed at influencing audiences and decision makers, like military deception, psychological operations, Civil Affairs, OPSEC, PA, etc.

One challenge to this recommendation is that the commander of USCYBERCOM also serves as the Director of the National Security Agency. This reorganization could be synchronized with the termination of the dual-hatted arrangement of the commander of USCYBERCOM as the Director of the National Security Agency as well. National Defense Authorization Act for the fiscal year 2017 outlines the requisite conditions for this termination. If the conditions are not yet suitable for termination, then the

commander of the joint cyber component commander, the Deputy Commanding General-Cyber, depicted in figure 10 can remain dual-hatted in accordance with national guidance until the separation can occur.

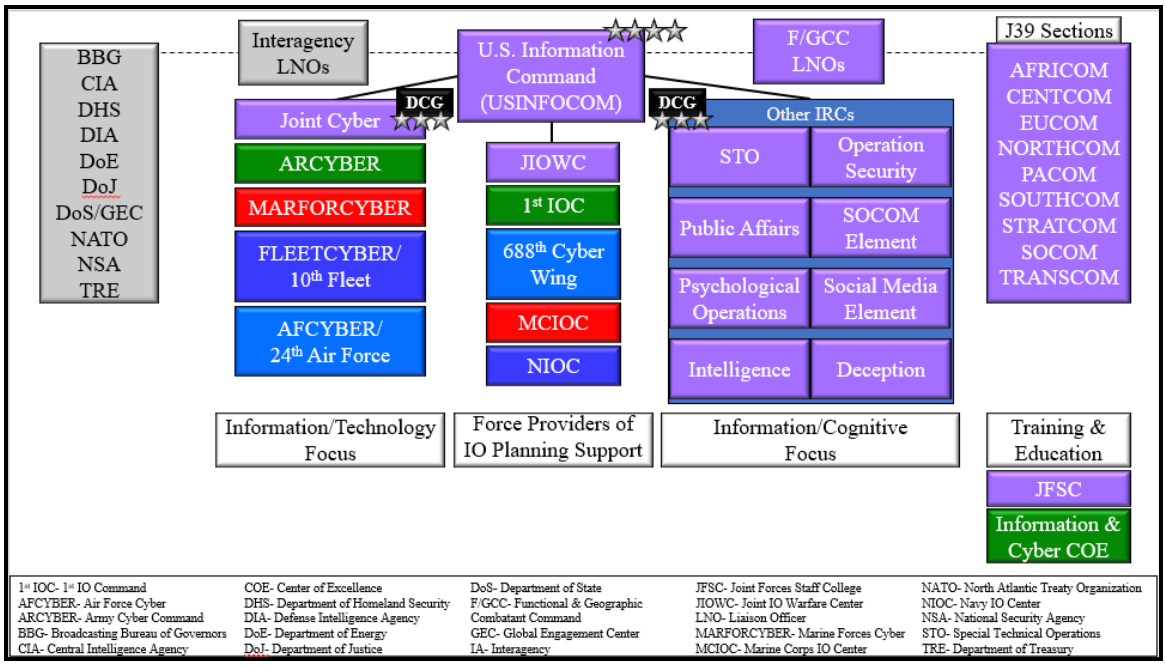


Figure 10. Proposed organizational structure of Information Command

Source: Created by author.

Under the Influence side of this combatant command, there would be a unique psychological operations battalion separate from those subordinates to 1st Special Forces Command. A rotationally deploying psychological operations battalion serving as a Joint Military Information Support Operations Task Force would not work in this restructure as the supporting battalion would need to be capable of providing support to all GCCs rather than being experts in a single region, as is the case with most of the MISO battalions.

Deception units and social media entities could be aligned under the USINFOCOM as well.

Another beneficial aspect of geography for this proposition is that three of the four service IO commands reside in the National Capital Region: Army, Marine Corps, and Navy. Also, the commanders and staffs would be in proximity to the Pentagon and many of the interagency enterprises to facilitate better coordination and synchronization of efforts and operations in the IE, as directed in the guidance issued in 2016 by then-Secretary of Defense Ash Carter.[93] Alignment of the service IO commands under USINFOCOM would support this guidance.

Furthermore, the value of open source intelligence cannot be understated. Resident in proposed USINFOCOM needs to be a capability to monitor open source digital and social media that employ data aggregation and possibly artificial intelligence or other algorithms to provide assessments and sentiment analysis. This capability would better inform commanders and decision makers at DoD and USG levels. It could also observe indicators of the effectiveness of ongoing information operations or cue additional information operations to preserve or regain strategic initiative in the IE.

A USINFOCOM functional combatant command with organic IRC subordinate staffs and organizations could address many gray zone activities in conjunction with United States Special Operations Command and GCCs to counter Russian threats, and other identified adversaries, at the strategic level. This command could also provide reach back support to forward-deployed Joint Task Forces and GCCs that require operational

[93] Department of Defense, *Strategy for Operations in the Information Environment*, 14.

and tactical support in the IE. Such a structure could unify strategic military operations in the IE and foster better interoperability with the Department of State's Global Engagement Center, other governmental agencies, and international allied entities to counter Russian aggression in the IE. Therefore, despite the near-term difficulties this recommendation presents, the DoD should consider the long-term strategic benefits of the proposed organizational restructuring of USCYBERCOM. The proposed restructuring would allow the DoD to conduct effective operations in the IE against state and non-state actors alike.

The second organizational recommendation is to reactivate an army tactical deception unit akin to the 23rd Special Troops from World War II. This establishment or reactivation would set conditions for future large-scale combat operations against an adversary like Russia. While this unit would require additional capabilities to account for advanced technology on the battlefield, the concept remains valid. The theater army should control this unit, and the theater commander would provide the unit with priorities of support for subordinate units. Inherent in the new capabilities would be social media exploitation and authority to conduct operations in the IE within the theater commander's intent

The third organizational recommendation is to add an FA30 back into brigade combat teams or modify to unit tables of organization and equipment of maneuver brigades to add a requirement for certain positions in the operations and intelligence staff directorates have the IO qualification. There are multiple Information Capability Specialists organic to an army brigade, but no professional IO officer to coordinate and integrate their employment in support of the commander's plan. It is ludicrous to proffer

that a staff officer without formal IO training from the operations staff section would assume the duties of the IO officer in addition to what their billet calls for- especially with the complexity of the IE and the potential strategic ramifications of a misstep at the tactical level. Further, the officers in that section are likely from CGSC or the Captain Career Course and are not educated adequately to understand operations in the IE. The MISO, PA, or EW officers organic to brigades that might fill the role of IO officer are more likely to have a better understanding than maneuverists, but might tend toward their IRC specialty rather than on maximizing the breadth of capabilities that could be brought to bear.

Leadership Education

Finally, more emphasis on education must be a priority. Formally train operations and intelligence personnel in IO to generate a better understanding of IO in the across the warfighting functions, and to improve interoperability with IO planners on unit staffs to better plan and assess the effectiveness of operations in the IE. Education on IO cannot simply be an offered elective, but an ingrained part of the curriculum.[94] Satisfaction of this proposition can be an increase in the number of contact hours of instruction in IO and increase the integration of IO into exercises at PME. Additionally, the Army could institute a policy wherein select personnel attend the IO Qualification Course as a follow-on school upon graduation from CGSC before they move to their next units of assignment. Another option would be to bring a two-week mobile training team to the college to instruct select students on tactical IO planning, which upon graduation would

[94] Vertuli, interview by the author via telephone, Fort Leavenworth, KS, 25 April, 2018.

bestow the P4 additional skill identifier as a Tactical IO Planner. Any of these options will provide more awareness across the force.

Develop education programs for media literacy and online identity management for unit training, or at least part of initial entry training and PME, Installation Management Command provided cybersecurity and digital/social media identity management as part of OPSEC/protection aspect of defensive operations in the IE. This Installation Management Command provided training should be part of inprocessing at every DoD installation and be available to family readiness groups.

In the Information Age, will commanders be risk-averse to make timely decisions outside a high-intensity environment and opt to wait for more information? A mitigation for the recent trend toward information overload is to improve commander's and staff's ability to exercise the operational art. Joint doctrine defines the operational art as the "cognitive approach by commanders and staffs—supported by their skill, knowledge, experience, creativity, and judgment—to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, and means."[95] Through increased education on the IE, IO, and improved media literacy, servicemembers may be more likely to have more developed knowledge, creativity, and judgment.

While none of these recommendations are near-term solutions to addressing threats in the IE, that is the nature of IO. It takes time to see effects from IO and changing a military culture of technology and firepower to appreciate the implications of the IE is no different. If the DoD adopts any of these recommendations of doctrine, organization, and education reform, there will be a marked improvement of the force to compete with

[95] Joint Chiefs of Staff, JP 3-0 *Joint Operations* (2017), II-3.

adversaries, including Russia, in the IE at the different levels of warfare and throughout the spectrum of conflict.

Suggestions for future research

While the focus of this thesis was doctrine, organization, and leadership education, the DoD could benefit from research focused on capability gaps that exist in the training element of DOTMLPF-P with regards to IO. Another topic of research is to determine whether cyberspace is truly an operational domain, or should it be an information or cognitive domain? This topic arose multiple times during this research from document review and interviews.

Russia-focused research could include leveraging the Russia Information Group as a forward extension of a United States Information Agency 2.0 centered around the GEC or DoD. During this research, the author found that the DoS and EUCOM co-chair a Russia Information Group to "[establish] interagency awareness of each organization's priorities and efforts in identifying and combatting malign Russian influence in the information space."[96] This interagency entity seems an ideal prospect to take a whole-of-government approach to competing with Russia in the IE.

Even during this research, evidence emerged about Russian involvement in U.S. election meddling via social media campaigns on Twitter and Facebook. This reporting indicates that Russia will continue to wage NGW against the U.S. in a manner that is low cost with high return on investment. This approach would allow Russia to continue eroding U.S. military operational advantage by detracting from the political and military

[96] Michael Jackson, Congressional Information Paper: Russia Information Group (RIG), (White Paper, March 14, 2017).

readiness through gray zone activities, which is simply steady state information warfare for Russia. Through greater understanding of the IE, the military, the government, and society can better work in a unified manner towards securing national interests and develop a more resilient society against the disinformation campaigns of Russia and other adversaries.

GLOSSARY

Active Measures. Soviet-era term used to describe information, psychological, or political means conducted to advance Soviet foreign policy goals and extend influence throughout the world.

Capabilities-Based Assessment. Doctrine, Organization, Training, Materiel, Leader Education, Personnel, Facilities, and Policy (DOTMLPF-P). These terms are aspects of the analysis process to identify capabilities gaps as part of the DoD Force Management Process.

Covert action. Activity or activities of the United States Government to influence political, economic or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly.

Global Engagement Center. A forward-looking, innovative organization that can shift focus quickly to remain responsive to agile adversaries. The GEC leverages data science, cutting-edge advertising technologies, and top talent from the private sector. With detailees from across the interagency, the GEC coordinates messaging efforts to ensure they are streamlined and to eliminate duplication.

Gray Zone. Competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality.

Information Environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The IE consists of three dimensions: physical, informational, and cognitive.

Information Operations. The integrated employment, during military operations, of information-related capabilities, in concert with other lines of operation, to influence, disrupt, corrupt, or usurp the decisionmaking of adversaries, or potential adversaries, while protecting our own.

Information Warfare. The use of technical and influential means to influence an adversary to act against their own interests.

Information Related Capabilities. Tools, techniques, or activities employed within a dimension of the information environment that can be used to create effects and operationally desired conditions.

Informational instrument of national power. Information remains an important instrument of national power and a strategic resource critical to national security. Previously considered in the context of traditional nation-states, the concept of information as an instrument of national power extends to non-state actors—such as terrorists and transnational criminal groups—that are using information to further their causes and undermine those of the USG and our allies. DOD operates in a

dynamic age of interconnected global networks and evolving social media platforms. Every DOD action that is planned or executed, word that is written or spoken, and image that is displayed or relayed, communicates the intent of DOD, and by extension the USG, with the resulting potential for strategic effects.

Instruments of National Power: Diplomatic, Informational, Military, Economic. These terms represent the U.S. instruments of national power.

Military Information Support Operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives.

Perception Management. Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations. (Joint Pub 3-13; 1998)

Propaganda. An activity within the range of covert action; political technique of disseminating information that has been created with a specific political outcome in mind; used to support individuals or groups friendly to one's own side or to undermine one's opponents; can also be used to create false rumors of political unrest, economic shortages, or direct attacks on individuals.

Reflexive Control. A means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action.

Sharp Power. The deceptive use of information for hostile purposes; a type of hard power which pierces, penetrates, or perforates the political and information environments in the targeted countries.

Social Media. Means of interaction within the cyber domain among users in which they create, share, and exchange information and ideas in virtual communities and networks.

Soft Power. A persuasive approach to international relations, typically involving the use of economic or cultural influence to change behavior through attraction, distinct from overt diplomatic or military coercion.

Unconventional Warfare. Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by

operating through or with an underground, auxiliary, and guerrilla force in a denied area.

U.S. Information Agency. Cold War era agency responsible for monitoring and influencing opinion abroad of the United States and its objectives.

APPENDIX A

CGSC INFORMATION OPERATIONS INSTRUCTION SURVEY

"This survey will provide data on possible gaps in Information Operations (IO) capabilities with regard to doctrine, organizations, training, and leadership education via Professional Military Education. Your input and feedback will be valuable to identifying gaps and informing possible solutions to improve overall efforts in the operational and information environments to support commanders.

This survey is voluntary and anonymous. The requested personal information will provide context to your response but will not identify you. Provision of this information is voluntary but will enhance the analysis of responses. This personal data will not be shared outside of this study and will be destroyed upon its completion. The researcher will not make any attempt to identify you from your administrative data or your responses.

Do not discuss For Official Use Only or classified information in this survey. All responses must be unclassified.

By clicking "Next" you affirm your consent to participate in this survey and will adhere to the conditions stated above.

If you have any questions regarding this request for consent and this survey, contact CPT Nicholas Kane at nicholas.j.kane6.mil@mail.mil"

Q1: The formal instruction I received on Information Operations at Professional Military Education has been sufficient. Why?

Likert Scale: Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree
Free Response:

Q2: The addition of Information as a Joint Function in JP 3-0 is clearly defined. Why?

Likert Scale: Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree
Free Response:

Q3: Information Operations personnel serve under which staff directorate?
Multiple Choice.

a. G/J2
b. G/J3
c. G/J5
d. G/J6

e. G/J7

Q4: I had a good understanding of Information Operations prior to attending Command & General Staff College. Why?

Likert Scale: Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree
Free Response:

Q5: Understanding of the information environment and incorporation of the information joint function into the MDMP scenarios in AOC were sufficient. Why?

Likert Scale: Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree
Free Response:

Q6: What is the definition of Information Operations, in your own words?
Free response

Q7: What is the difference between the roles of Public Affairs and Military Information Support Operations (MISO, formerly called PSYOP)
Free Response

Q8: What do you perceive the problems with IO and doctrine are?

Q9: What do you think are the most significant concerns/issues with Information Operations? Why?
Free Response

APPENDIX B

BIOGRAPHIES OF INTERVIEWEES

MG Gordon B. “Skip” Davis Jr. is currently the J3 (Director of Operations) for the United States European Command. His previous NATO assignments include Deputy Chief of Staff, Operations and Intelligence, SHAPE; Deputy Chief of Staff Operations and Intelligence, Allied Rapid Reaction Corps; ISAF Joint Command CJ5. Most of MG Davis’s career has been spent in Europe with assignments in Italy, France, Germany, Great Britain, and Belgium.

COL Michael Jackson is currently the United States European Command J-39, and previously served as the Special Operations Command Europe J-39. He has been an Army Information Operations Officer since 2003.

COL Mark Vertuli is currently the United States Strategic Command J-35, and previously served as the Special Operations Command Europe J-39, and as the 1st Bn, 1st IOC Commander. He has been an Army Information Operations Officer since 2005.

MAJ Jerome Peterson is currently a doctrine writer at the Combined Arms Doctrine Directorate at Fort Leavenworth, Kansas. He has been an Army Information Operations Officer since 2010.

LTC Amy Burrows is currently a Command and General Staff School Instructor in the Department of Joint, Interagency, Multinational Operations. She has been a PSYOP officer since 2007.

BIBLIOGRAPHY

Armistead, Leigh. *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington, DC: Brassey's, 2004.

Boston, Scott, and Dara Massicot. *The Russian Way of Warfare: A Primer*. Santa Monica, CA: RAND Corporation, 2017.

Breedlove, Philip M. "How to Handle Russia and Other Threats." *Foreign Affairs*, 13 June 2016. Accessed 25 April, 2018. https://www.foreignaffairs.com /articles/europe/2016-06-13/natos-next-act.

Burnore, Nathanael. "Social Media Application for Unconventional Warfare." Master's thesis, Command and General Staff College, Fort Leavenworth, KS, 2013.

Center for Army Lessons Learned. CALL Handbook No. 17-09, *Russian New Generation Warfare.* Fort Leavenworth, KS: Center for Army Lessons Learned, 2017.

Center for Strategic International Studies: Russia and Eurasia Program. "The Ukraine Crisis Timeline." Accessed 21 February 2018, http://ukraine.csis.org /crimea.htm#6

Chairman of the Joint Chiefs of Staff. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01C, *Joint Information Operations Proponent*. Washington, DC: Government Printing Office, 2014.

Darczewska, Jolanta "Russia's Armed Forces on the Information War Front: Strategic Documents." OSW Studies, Warsaw, June 2016.

David, G. J., and T. R. McKeldin III, ed. *Ideas as Weapons: Influence and Perception in Modern Warfare*. Washington, DC: Potomac Books, 2009.

Davitch, James M. "Open Sources for the Information Age: Or How I Learned to Stop Worrying and Love Unclassified Data." *Joint Forces Quarterly*, no. 87 (4th Quarter 2017): 18-25.

Department of Defense. *Strategy for Operations in the Information Environment*. Washington, DC: Government Printing Office, 2016.

———. *Summary of the 2018 National Defense Strategy of the United States of America*. Washington, DC: Government Printing Officer, 2018.

Department of State. "Global Engagement Center." Accessed 27 October, 2017. https://www.state.gov/r/gec/.

Department of the Army. Army Doctrine Reference Publication (ADRP) 6-0, *Mission Command.* Washington, DC: Government Printing Office, 2012.

———. Field Manual (FM) 3-0, *Operations*, Change 1. Washington, DC: Government Printing Office, 2017.

———. Field Manual (FM) 3-0, *Operations*. Washington, DC: Government Printing Office, 2008.

———. Field Manual (FM) 3-13, *Information Operations*. Washington, DC: Government Printing Office, 2016.

———. Field Manual (FM) 3-13, *Inform and Influence Activities*. Washington, DC: Government Printing Office, 2013.

———. Field Manual 100-6, *Information Operations*. Washington, DC: Government Printing Office, August 1996.

Dubik, James W., and Nic Vincent. *America's Global Competitions: The Gray Zone in Context*. Washington, DC: Institute for the Study of War, 2018.

Fox, Amos, and Andrew Rossow. *Making Sense of Russian Hybrid Warfare: A Brief Assessment of the Russo Ukrainian War.* Arlington, VA: Institute of Land Warfare, 2017.

Gawne, Jonathan. *Ghosts of the ETO: American Tactical Deception Units in the European Theater of Operations 1944-1945*. Havertown, PA: CASEMATE, 2002.

Harr, Scott. "Expanding Tolstoy and Shrinking Dostoyevsky: How Russian Actions in the Information Space are Inverting Doctrinal Paradigms of Warfare." *Military Review* (September-October 2017): 39-48.

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, Zev Winkelman. *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*. Santa Monica, CA: RAND Corporation. 2018.

Новиков, В.К., С.В. Голубчиков. Вестник, Вестник, 3 (60), 2017, стр. 10-16. [V. K. Novikov and S. V. Golubchikov. "Color Revolutions in Russia: Possibility and Reality." *Vestnik,* 3 (60) (2017): 10-16].

Hodne, David. "Accruing Tacit Knowledge: A Case for Self-Study on behalf of Professional #Leadership." The Strategy Bridge, 3 April 2016. Accessed 26 April 2018. https://thestrategybridge.org/the-bridge/2016/4/3/accruing-tacit-knowledge-a-case-for-self-study-on-behalf-of-professional-leadership.

Houghton, Nicholas. “Building a British Military Fit for Future Challenges Rather Than Past Conflicts.” Transcript of speech made by General Sir Nicholas Houghton, Chatham House, London, 15 September 2015. Accessed 25 April 2018. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150901-Chatham%20House%20Speech-O.pdf.

Jackson, Michael. Congressional Information Paper: Russia Information Group (RIG), White Paper, March 14, 2017.

Joint Chiefs of Staff. Joint Doctrine Note 2-13, *Commander’s Communication Synchronization*. Washington, DC: Government Printing Office, 2013.

———. Joint Publication (JP) 1-0, *Doctrine for the Armed Forces of the United States*. Washington, DC: Government Printing Office, 2013.

———. Joint Publication (JP) 1-0 *Doctrine of the Armed Forces of the United States*, change 1. Washington, DC: Government Printing Office, 2017.

———. Joint Publication (JP) 1-02, *Dictionary of Military and Associated Terms*. Washington, DC: Government Printing Office, 2010.

———. Joint Publication (JP) 3-13, *Information Operations*, Change 1 Washington, DC: Government Printing Office, 2014.

———. Joint Publication (JP) 3-0, *Joint Operations*. Washington, DC: Government Printing Office, 2006.

———. Joint Publication (JP) 3-0, *Joint Operations*. Washington, DC: Government Printing Office, 2017.

Lowe, Christopher. “The ‘Battle’ and the ‘Battle of Ideas’: Misunderstanding of Information.” Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2010.

Marler, Scott. “Russian Weaponization of Information and Influence in the Baltic States.” Master’s Thesis, Command and General Staff College, Fort Leavenworth, KS, 2017.

Naval Information Operations Command. “Homepage.” Accessed 28 March 2018. http://www.public.navy.mil/fltfor/niocnorfolk/Pages/default.aspx/.

Nye, Joseph, “Get Smart-Combining Hard and Soft Power.” *Foreign Affairs* 88, no. 4 (July/August 2009): 160-163.

———. “How Sharp Power Threatens Soft Power: The Right and Wrong Ways to Respond to Authoritarian Influence.” *Foreign Affairs,* 24 January, 2018. Accessed 19 February, 2018. https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power?cid=int-fls&pgtype=hpg&utm_source=Sailthru&utm_medium=email&utm_campaign=ebb%2001.25.2018&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief.

Nye, Joseph, and William A. Owens. “America’s Information Edge” *Foreign Affairs*, March 1996. Accessed 25 April, 2018. https://www.foreignaffairs.com/articles/united-states/1996-03-01/americas-information-edge.

Polykova, Alina, and Spencer P. Boyer. *The Future of Political Warfare: Russia, The West, and the Coming of Age of Global Digital Competition*. Washington, DC: Brookings Institute, 2018.

Pomerantsev, Peter, and Michael Weiss. *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture, and Money*. New York: The Institute of Modern Russia, 2014.

President of the United States. *National Security Strategy of the United States of America*. Washington, DC: The White House, 2017.

Rathke, Jeffrey. “Can NATO Deter Russia in View of the Conventional Military Imbalance in the East?” Center for Strategic and International Studies, 30 November 2015. Accessed 22 March 2017. https://www.csis.org/analysis/can-natodeter-russia-view-conventional-military-imbalance-east.

Rid, Thomas, and Marc Hecker. *War 2.0*: *Irregular Warfare in the Information Age*. Westport, CT, Praeger Security International, 2009.

Rothenberger, Liane. “Terrorist Groups: Using Internet and Social Media for Disseminating Ideas.” *Romanian Journal of Communication and Public Relations* 3 (March 2012): 7-23.

Scharre, Paul. “Readying the U.S. Military for Future Warfare.” Testimony before the House Armed Services Committee, 30 January 2018. Accessed 23 March, 2018. https://www.cnas.org/publications/congressional-testimony/paul-scharre-testimony-before-hasc-2.

Schoen, Fletcher, and Christopher J. Lamb. *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*. Strategic Perspectives 11. Washington, DC: National Defense University, 2012.

Secretary of Defense. *Guidance from Secretary Jim Mattis*. Washington, DC: Government Printing Office, October 2017.

Sinclair, Nick. “Old Generation Warfare: The Evolution-Not Revolution-Of the Russian Way of War.” *Military Review* 96, no. 3 (May/June 2016): 8-16.

Snegovaya, Maria. *Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare*. Washington, DC: Institute for the Study of War, 2015.

Steele, Robert David. “Information Operations: Putting the “I” back in DIME.” Report, Strategic Studies Institute, Carlisle, PA, 2006.

Sutyagin, Igor, and Justin Bronk. “Russia’s New Ground Forces: Capabilities, Limitations and Implications for International Security.” Whitehall paper, RUSI, 2017.

Tenth Fleet/Fleet Cyber Command. “Homepage.” Accessed 28 March, 2018. www.public.navy.mil/fcc-c10f/Pages/home.aspx.

Thomas, Timothy L. *Kremlin Kontrol: Russia’s Political-Military Reality*. Fort Leavenworth, KS: Foreign Military Studies Office, 2017.

———. *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness*. Fort Leavenworth, KS: Foreign Military Studies Office, 2011.

———. *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics*. Fort Leavenworth, KS: Foreign Military Studies Office, 2015.

———. “Russia’s Reflexive Control Theory and the Military.” *Journal of Slavic Military Studies* 17 (2004): 237-256. DOI: 10.1080/13518040490450529.

Truman, Harry S. “Address on Foreign Policy at a Luncheon of the American Society of Newspaper Editors.” 20 April, 1950. Accessed 29 April, 2018. http://www.presidency.ucsb.edu/ws/index.php?pid=13768.

Tsygankov, Andrei P. “Foreign Policy and Relations with the United States.” In *Putin’s Russia: Past Imperfect, Future Uncertain,* edited by Stephen K. Wegren, 233-255. 6th ed. Lanham, MD: Rowman and Littlefield, 2016.

U.S. Army Special Operation Command. *Little Green Men: A Primer on Modern Russian Unconventional Warfare Ukraine 2013-2014*. Fort Bragg, NC: Special Operations Command, 2016.

U.S. Congress. House. *Countering Foreign Propaganda and Disinformation Act of 2016*. H.R.5181.

———. *Crafting an Information Warfare and Counter-Propaganda Strategy for the Emerging Security Environment.* Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services, 115th Cong., 1st Sess., 15 March 2017.

U.S. Fleet Cyber Command. “Homepage.” Accessed 29 April, 2018. www.public.navy.mil/fcc-c10f/Pages/home.aspx.

U.S. Marine Corps. MCRP 1-10.2 (formerly MCRP 5-12C), *Marine Corps Supplement to the DOD Dictionary of Military and Associated Terms*. Washington, DC: Government Printing Office, August 2013.

———. MCWP 3-40.4, *Marine Air Ground Task Force Information Operations*. Washington, DC: Government Printing Office, 2013.

Van Herpen. Marcel H. *Putin’s Propaganda Machine: Soft Power and Russian Foreign Policy.* Lantham, MD: Rowman and Littlefield, 2016.

———. *Putin’s Wars: The Rise of Russia’s New Imperialism*, 2nd ed. New York: Rowman and Littlefield, 2015.

Velez-Green, Alexander. “The United States and Russia Are Already at War.” *Small Wars Journal*. Accessed 26 April, 2018. http://smallwarsjournal.com/jrnl/art/the-united-states-and-russia-are-already-at-war.

Vertuli, Mark D. “A Myth Retold: The Army’s MILDEC Program in the 21st Century.” *IO Sphere* (Fall 2015): 19-24.

Walker, Christopher, and Jessica Ludwig. “The Meaning of Sharp Power: How Authoritarian States Project Influence.” *Foreign Affairs,* 16 November 2017. Accessed 26 April, 2018. https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power.

Zygar, Mikhail. “The Russian Reset That Never Was.” *Foreign Policy*, 9 December 2016. Accessed 29 November 2017. http://foreignpolicy.com/2016/12/09/the-russianreset-that-never-was-putin-obama-medvedev-libya-mikhail-zygar-all-the-kremlinmen/amp/.